Methodische Modellierung und Analyse von Sicherungssystemen des Eisenbahnverkehrs

Von der Fakultät für Maschinenbau
der Technischen Universität Carolo-Wilhelmina zu Braunschweig
zur Erlangung der Würde eines Doktor-Ingenieurs (Dr.-Ing.)
genehmigte Dissertation

von:	Ing. Roman Slovák
aus:	Martin

eingereicht am:	13. Juni 2006
mündliche Prüfung am:	25. Juli 2006
Referenten:	Prof. Dr.-Ing. Dr. h.c. E. Schnieder
	Prof. Dr.-Ing. B. Bertsche
Vorsitzender:	Prof. Dr.-Ing. K. Lemmer

2006

Vorwort

Die vorliegende Arbeit entstand großenteils während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Institut für Verkehrsicherheit und Automatisierungstechnik der Technischen Universität Braunschweig. An dieser Stelle möchte ich mich bei allen bedanken, die zum Gelingen der Arbeit beigetragen haben.
An erster Stelle gilt mein Dank dem Leiter des Instituts Herrn Professor Eckehard Schnieder, für die Betreuung und Förderung der Arbeit. Ich schätze sehr sein ständig großes Interesse, seine kompetente und konstruktive Unterstützung mit vielen Hinweisen und Anregungen sowie sein menschliches Verständnis während des engen Zeitplans der Abschlussphase.
Auch Herrn Professor Bernd Bertsche (Universität Stuttgart) danke ich herzlich für sein Interesse an meiner Arbeit und die unkomplizierte und kompetente Durchführung der Mitberichterstattung. Ebenso möchte ich mich bei Herrn Professor Karsten Lemmer (Deutsches Zentrum für Luft- und Raumfahrt) für die Übernahme des Vorsitzes bedanken.
Bedanken möchte ich mich auch bei allen meinen Kolleginnen und Kollegen die zu meiner Arbeit beigetragen haben. Meinem Kollegen Stefan Wegele danke ich für seine ständige und allseitige Unterstützung. Besonderer Dank geht auch an die ehemaligen Kollegen Stefan Einer und Michael Meyer zu Hörste, die durch unzählige Diskussionen sowie durch deren eigene Arbeiten meine Arbeit motiviert und geformt haben. Dem Kollegen Jörg R. Müller danke ich für viele petrinetztheoretische Aufklärungen sowie seine hervorragenden Sprachkorrekturen. Für diese möchte ich mich auch bei Frau Regine Stegemann sehr herzlich bedanken.
Mein Dank geht auch an Mitarbeiter des Lehrstuhls für Steuerungs- und Informationssysteme der Universität Žilina in meiner Heimat, deren praktische Erfahrungen das Thema meiner Arbeit in Ihrem Anfang stark geprägt haben. Namentlich möchte ich an dieser Stelle Herrn Professor Pavol Tomašov, Herrn Professor Jiří Zahradník und Herrn Dozent Karol Rástočný erwähnen sowie auch Herrn Dozent Vojtech Šoltýs, der als Betreuer mich erstes Mal an die Mächtigkeit der Modellierung mit Petrinetzen aufmerksam gemacht hat.
Nicht zuletzt danke ich meinen Eltern, die mir meine Ausbildung ermöglichten und meiner Freundin Lora El Kadri, die mich mit viel Liebe und Geduld in dieser Zeit unterstützt hat.

Braunschweig, im Dezember 2006

Roman Slovák

Inhaltsverzeichnis

Abkürzungsverzeichnis

AEG	Allgemeines Eisenbahngesetz
AEIF	Association Européen d'Interopérabilité Ferroviaire
ALARP	As Low As Reasonably Practicable
ATP	Automatic Train Protection
BE-Netz	Bedingungs-Ereignis-Netz
BÜ	Bahnübergang
BÜSA	Bahnübergangssicherungsanlage
CENELEC	Comité Européen de Normalisation Electrotechnique
CPN	Colored Petri Nets
CSI	Common Safety Indicator
CSM	Common Safety Method
CST	Common Safety Target
DC	Decomposition
DFG	Deutsche Forschungsgemeinschaft
DZ	Danger Zone
EBO	Eisenbahn-Bau- und Betriebsordnung
EDSPN	Extended Deterministic and Stochastic Petri-Nets
ELSS	Eisenbahnleit- und Sicherungssysteme
ETA	Event Tree Analysis
F-Plätze	Plätze der Systemfunktionalität
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode and Effect Criticality Analysis
FTA	Fault Tree Analysis
GAME	Globalement Au Moins Equivalent
GAMAB	Globalement Au Moins Aussi Bon
GSPN	General Stochastic Petri Nets
H-Plätze	Platz des gefährlichen Ausfalls (Hazard)
HAZOP	Hazardous Operation Analysis
HCPN	Hierarchical Colored Petri Nets

HceFS	Hazard-Bedingung/Aufforderung-Fail-Safe
HceI	Hazard-Bedingung/Aufforderung-Intakt
HcetFS	Hazard-Bedingung/Aufforderung/Zeitdauer-Fail-Safe
HcetI	Hazard-Bedingung/Aufforderung/Zeitdauer-Intakt
HctFS	Hazard-Bedingung/Zeitdauer-Fail-Safe
HctI	Hazard-Bedingung/Zeitdauer-Intakt
HeFS	Hazard-Zeitdauer-Fail-Safe
HeI	Hazard-Aufforderung-Intakt
HetFS	Hazard-Aufforderung/Zeitdauer-Fail-Safe
HetI	Hazard-Aufforderung/Zeitdauer-Intakt
HtI	Hazard-Zeitdauer-Intakt
I-Plätze	Plätze der Systemimplementierung
IcFS	Intakt-Bedingung-Fail-Safe
IcH	Intakt-Bedingung-Hazard
ItFS	Intakt-Zeitdauer-Fail-Safe
ItH	Intakt-Zeitdauer-Hazard
K^2	Korrelationsfaktor
LC	Level Crossing
MEM	Minimale Endogene Mortalität
$MEM_{CENELEC}$	Akzeptanzwert nach EN 50126
MGS	Mindestens Gleiche Sicherheit
NMAU	Nicht Mehr Als Unvermeidbar
P-Plätze	Plätze des Prozessmodells
PROFUND	Process, Functionality, Dependability
R	Risiko
RAMS	Sicherheit, Zuverlässigkeit, Verfügbarkeit und Instandhaltbarkeit
LZ	Lichtzeichen
ZE	Zugerkennung
STG	Steuerung
RBD	Reliability Block Diagrams
RS (=EG)	Reachability Set
SIL	Sagety Integrity Levels
SPAD	Signal Passed At Danger
TC	Track Circuit
TFSR	Tolerable Fail-Safe Rate
THr	Tolerierbare Hazardrate
TRC	Train-Route-Control
UML	Unified Modelling Language
V-Plätze	Plätze des Verlässlichkeitsmodells

Kurzfassung

Derzeit werden in den europäischen Ländern noch unterschiedliche organisatorische Strukturen, Strategien und betriebliche Regeln genutzt, um einen sicheren Eisenbahnverkehr zu gewährleisten. Der gemeinsame europäische Markt und die Anforderung an die Interoperabilität führen zum Bestreben nach Harmonisierung. Aus diesem Grund wurden von der CENELEC die ersten europäischen Normen erarbeitet, die die Verlässlichkeit im Sinne eines Oberbegriffes für Sicherheit, Zuverlässigkeit, Verfügbarkeit und Instandhaltbarkeit (RAMS) der Eisenbahnleit- und -sicherungssysteme betreffen. Im Gegensatz zum früher eher absoluten Verständnis der Sicherheit, basiert die neue Definition der Normen auf der Akzeptanz eines zulässigen Risikos des Eisenbahnbetriebes. Es ist eine Aufgabe der Sicherheitsanalyse, das betriebliche Risiko zu ermitteln und auf seiner Basis die Anforderungen und Sicherheitsziele an die Betrieb steuernden und sichernden technischen Systeme zu definieren.

Die geltenden Normen sind allgemein gefasst und schreiben nicht konkret ein methodisches Vorgehen oder Regeln zur Ableitung von Sicherheitsanforderungen für Systemkomponenten aus dem zulässigen betrieblichen Risiko vor. Für diese Herleitung wird nur eine Reihe von mehr oder weniger formalen Techniken empfohlen und mit unterschiedlichem Erfolg eingesetzt. In den einzelnen Entwicklungsschritten werden meist verschiedene Systemmodelle und Beschreibungsmittel verwendet. Diese sind oft nicht systematisch ineinander überführbar, was das Risiko von Entwicklungsfehlern deutlich erhöht und die Nachvollziehbarkeit und die Transparenz des Entwurfs verringert.

Um eine ausreichende Genauigkeit der Risikobewertung zu erreichen, ist ein holistischer Ansatz der Beschreibung aller beitragenden Risikofaktoren notwendig. Das grundlegende Konzept der in dieser Arbeit angewendeten *PROFUND*-Methode zur Sicherheitsanalyse von Eisenbahnsystemen sieht vor, für alle Einflussfaktoren des Risikos im Eisenbahnbetrieb ein einziges formales Beschreibungsmittel zu verwenden. Dieses betrifft einerseits den gesteuerten Verkehrsprozess (**Pro**ces), in welchem das Potential für Auftritt von unerwünschten Ereignissen besteht, anderseits die Funktionalität (**Fun**ctionality) und Verlässlichkeit (**D**ependability) des untersuchten Eisenbahnleit- und -sicherungssystems.

Ziel dieser Arbeit ist zu zeigen, wie die Nutzung eines formalen Beschreibungsmittels

die risikobasierte Sicherheitsanalyse methodisch unterstützen kann. Als geeignete formale Notation wurden Petrinetze gewählt. Diese Wahl wurde einerseits durch einen ausgereiften mathematischen Hintergrund und breite Analysemöglichkeiten begründet, die bereits zu vielen praktischen Anwendungen geführt haben, andererseits durch deren Universalität. Das wichtigste Ziel der Arbeit ist es, die methodische Anwendung des Beschreibungsmittels dem Leser soweit wie möglich nahe zu bringen. Neben der Darstellung des Nutzungspotentials der formalen Herangehensweise, wurde darauf geachtet, den Bezug zum traditionellen Vorgehen beizubehalten und den formalen Ansatz als seine mögliche Erweiterung mit erkennbarem Mehrwert zu sehen.
Die Arbeit zeigt im Detail, wie die Petrinetze einerseits zur Beschreibung der Unfallschwere und andererseits der Unfallursachen aus dem Eisenbahnbetrieb, Systemverlässlichkeit oder Systemimplementierung eingesetzt werden können. Die parallele Anwendung der einzelnen Schritte des vorgestellten methodischen Vorgehens an Beispielen aus dem Eisenbahnbereich unterstützt die allgemeingültigen Ausführungen mit praxisnahen Erklärungen. Abschließend wird die vorgestellte *PROFUND*-Methode auf dem Beispiel der Definition der Sicherheitsanforderungen für ein Bahnübergangssicherungssystem vorgestellt.

Kapitel 1

Einleitung

Die Sicherheit gehört zu den Grundanforderungen an den Eisenbahnverkehr, der das Ziel hat, Menschen sowie Güter zu befördern. Diese Systemeigenschaft erwartet jeder Benutzer als Grundvoraussetzung, ohne sich dabei bewusst zu werden, was sich alles an Technischem und Organisatorischem hinter der Realisierung dieser Erwartung verbirgt. Die mehr als 150-jährige Geschichte dieses Verkehrsmittels hat mehrmals gezeigt, zu welchen Folgen die Vernachlässigung der Sicherheit führen kann. Die spektakulären Unfälle waren die beste Motivation für die Entwickler, sich im Rahmen der Systementwicklung neben den betrieblichen und technischen Aspekten auch ausreichend der Frage der Sicherheit zu widmen. So wurden einerseits Methoden entwickelt, mittels deren Anwendung die potentiellen negativen Folgen bestimmter Systemfehlzustände aufgedeckt werden können, anderseits typische technische Vorkehrungen, die ermöglichen, diese Folgen zu vermeiden, ohne dabei zu fordern, die Zuverlässigkeit der Systemkomponenten unbedingt erhöhen zu müssen. Die besten und am häufigsten angewendeten Prinzipien und Vorgehensweisen bildeten die Basis für die Standardisierung im Entwicklungsprozess von sicherheitsrelevanten Systemen des Eisenbahnwesens.

1.1 Legislativer Hintergrund

Seit vielen Jahren existieren in den meisten Ländern nationale Regelwerke, die dort Entwicklung, Bau und Betrieb der Eisenbahnleit- und -sicherungssysteme (ELSS) vorschreiben. Ein gemeinsamer Aspekt der Regelwerke ist das Ziel, auch im Falle eines Ausfalles nie in einen Zustand zu geraten, der für den Eisenbahnbetrieb eine Gefährdung darstellt (so genanntes *fail-safe* Prinzip). Die Ausnutzung der unzweifelhaften natürlichen Gesetze im Systemdesign wie die Gravitation, Undurchlässigkeit der Materie oder Entstehung eines magnetischen Feldes um Stromleiter herum, sowie Verwendung der Systemredundanz, bildete die Basis der Annahmen eines tolerierbaren Risikos im

Eisenbahnbetrieb. Es wurde allgemein so interpretiert, dass durch Einhaltung dieser Regeln ein System als ausreichend sicher angenommen werden kann. Durch diese nationalen Regelwerke wurden also länderspezifische Sicherheitsstandards definiert. Diese aus den nationalen und gesellschaftlichen Entwicklungen hervorgegangenen verschiedenen Sicherheitsphilosophien, die zu unterschiedlichen bis hin zu widersprechenden Anforderungen an die technische Ausstattung von Fahrzeugen oder den Betrieb führen, stellten das größte Hemmnis auf dem Weg zu einem europäischen Eisenbahnnetz dar.
In den 90er Jahren wurde im Rahmen einer Harmonisierung in Europa erkannt, dass eine solche Definition von scheinbar absoluter Sicherheit nicht als Basis für die weitgehende Einführung einer gemeinsamen Sicherheitskultur dienen kann [Mueller und Schnieder 2006]. Aus diesem Grunde wurde eine Reihe von Europäischen Normen für den gesamten Eisenbahnbereich geschaffen. Sie führen ein System abgestufter Sicherheit ein, das auf der Risikoauswertung basiert. Dies erfolgt zusammen mit bestimmten technischen Anforderungen und Prozessen zur Festsetzung und Überwachung einer hinreichenden Sicherheit über den gesamten Lebenszyklus einer Eisenbahnanlage oder eines Eisenbahnfahrzeuges [Stanley und Stutzbach 2006].
Diese Aspekte werden hauptsächlich durch die folgenden europäischen Normen abgedeckt:

EN 50126 Diese Norm [EN50126 1996] ist eine Haupt-Norm, die sich auf die Gesichtspunkte der RAMS (engl.: Reliability, Availability, Maintainability, Safety) eines Systems und den gesamten Lebenszyklus jeder Komponente und jedes Systems im Zusammenhang mit dem Eisenbahnverkehr bezieht. Sie legt die einzelnen Phasen dieses Zyklus wie Systemdefinition, Risikoanalyse, Ableitung der Sicherheitsanforderungen sowie deren Zuteilung bis auf die Systemkomponenten, Systemfertigung, -installation, -abnahme, sowie Systembetrieb bis zu der Stilllegung des Systems fest. Die Sicherheit ist definiert als *Nichtvorhandensein eines unzulässigen Schadensrisikos*. Der Anhang der Norm beinhaltet Vorschläge für Risikotoleranzkriterien, durch die ein vorhandene Risiko im Eisenbahnbetrieb untersucht und beurteilt werden kann.

EN 50129 Diese Norm [EN50129 1998] beschreibt detailliert, welche Maßnahmen und Dokumentationen für die Erstellung eines Sicherheitsnachweises eines sicherheitsrelevanten elektronischen Systems der Eisenbahnsignaltechnik erforderlich sind. Die Anhänge dieser Norm beinhalten weitere Details über bestimmte Schritte zur Erstellung eines Sicherheitsnachweises. Der Geltungsbereich ist eindeutig begrenzt auf die Entwicklungsphase von Eisenbahnsignaltechnik. Im Gegensatz zur EN 50126 wird unterschieden zwischen generischen und anlagespezifischen Sicherheitsnachweisen und es wird eine Förderung zur Anwendung von exakten tolerablen Gefährdungsraten zur

Festlegung von Sicherheitslevels (Sagety Integrity Levels) SIL 0 bis 4 (abgeleitet von der IEC 65108 [IEC65108]) eingeführt.

EN 50128 Diese Norm [EN50128 1999] beinhaltet zusätzliche Anforderungen an den Entwicklungsprozess der Software für sicherheitsrelevante Systeme der Eisenbahn, die die programmierbare Elektronik enthalten.

EN 50159-1 und EN 50159-2 In diesen Normen [EN50159-1 1999, EN50159-2 1999] werden zusätzliche Anforderungen für die geschlossene und offene sicherheitsrelevante Datenkommunikation der Systeme der Eisenbahn definiert.

Sicherheitsrichtlinie 2004/49/EG Die Herausgabe dieser Sicherheitsrichtlinie durch die Europäische Kommission (*Safety Directive*) im Jahr 2004 [2004/49/EC 2004] repräsentiert einen weiteren Schritt zu Harmonisierung der Sicherheit des europäischen Eisenbahnverkehrs. Schwerpunkt der Richtlinie ist eine Einführung eines Sicherheitsmanagementsystems sowohl für die Betreiber von Eisenbahnfahrzeugen als auch von Infrastruktureinrichtungen. Ergänzend hierzu sieht die Richtlinie die Einführung von gemeinsamen Sicherheitszielen (Common Safety Targets - *CST*), Sicherheitsindikatoren (Common Saftey Indicators - *CSI*) und Sicherheitsmethoden (Common Safety Methods - *CSM*) vor.

Nationale Regelwerke Nach Paragraph 4 Abs. 1 des Allgemeinen Eisenbahngesetzes (AEG) [AEG] sind die Eisenbahnen in Deutschaland verpflichtet, ihren Betrieb sicher zu führen und die Eisenbahninfrastruktur, die Fahrzeuge und das Zubehör sicher zu bauen und im betriebssicheren Zustand zu halten. Zur Anleitung gehören die Aufstellung betriebsinterner Arbeitsanweisungen (z.B. Fahrdienstvorschrift) und die Aus- und Fortbildung der Mitarbeiter. Etwas konkreter ist die als Rechtsverordnung erlassene Eisenbahn-Bau- und Betriebsordnung (EBO) [EBO]. Sie beinhaltet eine Reihe von Vorschriften, deren Anforderungen durch die Bahnanlagen und Fahrzeuge erfüllt werden müssen, um den geforderten sicheren Betrieb zu gewährleisten. Im Falle fehlender Vorschriften für bestimmte Systeme der Eisenbahn wird hier auf die anerkannten Regeln der Technik verwiesen. Zu den anerkannten Regeln der Technik sind u.a. auch geltende technische Sicherheitsvorschriften und die internationalen Bedingungen (d.h. z.B. auch die EN Normen) zuzuordnen [Wittenberg 2002].

1.2 Problemanalyse

Alle hier erwähnten Normen bieten meistens ziemlich allgemeine Hinweise dafür, wie die sicherheitsrelevanten Systeme der Eisenbahn zu entwickeln sind und welche Methoden zum Nachweis von deren Sicherheit angewendet werde können. Letztendlich ist es die Aufgabe der Ingenieure aufgrund ihres Expertenwissens, ihrer Erfahrung und ihres Verständnisses des Systems mögliche Wirkungsketten, die zu negativen Folgen führen können, vorherzusagen. Ob man dabei die negativen Folgen der denkbaren Ausfälle der Systemkomponenten oder möglichen Ursachen des denkbaren unerwünschten Systemverhaltens analysiert (*bottom up*, bzw. *top down* Ansätze), hängt die Qualität der Analysenergebnisse immer von der Kreativität des einzelnen Ingenieurs ab. Die meisten durch die Normen genannten Methoden basieren auf einer mehr oder weniger informellen Beschreibung der Wirkungsketten, die keinerlei feste Beziehung mit der funktionalen oder technischen Spezifikation des Systems beinhalten. Dazu kommt die Tatsache, dass die formalen Spezifikationstechniken sich nur sehr langsam zum Stand der Technik entwickeln und dass die Analyse oft noch auf einer informellen (z.B. reiner Text) oder semiformalen (z.B. UML) Systembeschreibung basiert.

Dass eine solche Vorgehensweise für Analysefehler sehr anfällig ist, liegt nahe. Die Unfallanalysen zeigen, dass die meisten tatsächlich zu katastrophalen Folgen führenden Wirkungsketten kaum vorstellbar waren und dass sie nur in ganz speziellen Situationen des betrieblichen oder funktionalen Verhaltens des Eisenbahngesamtsystems auftreten konnten. Viele dieser Unfälle sind gerade bei einem Rückfallbetrieb vorgekommen, das heißt während der Zeit, in der eine oder mehrere Regelfunktionen mit weniger zuverlässigen Ressourcen (z.B. einem Mensch) ausgeführt worden sind. Bei immer steigender Komplexität der modernen Systeme der Eisenbahn, wo immer sehr viele Menschen an der Entwicklung beteiligt sind und die Vernetzung zwischen verschiedenen Hardware- und Softwarekomponenten häufig schwer zu überblicken ist, ist ein informales Vorgehen bei der Sicherheitsanalyse immer schwieriger und fehleranfälliger.

Eine starke Unterstützung bieten in dieser Hinsicht die formalen Notationen [Schnieder 1998, Schnieder 1999a, Schnieder 2000, Tarnai und Schnieder 2003, Schnieder und Tarnai 2004] die es erlauben, die Ursache-Wirkung Beziehungen in einem beschriebenen Verhalten eindeutig mathematisch zu beweisen. Da sich die aus dem Informatikbereich stammenden formalen Beschreibungsmittel meistens außerhalb der Ingenieurpraxis befinden, verbreitet sich deren Anwendung dort nur sehr langsam. Die häufigste hindernde Ursache breiterer praktischer Nutzung ist das Ausbleiben eines domänenspezifischen methodischen Vorgehens, das auch ohne mathematische Vorkenntnisse den praktischen Einsatz ermöglichen würde. Dazu kommt der zweite, ebenso wichtige Aspekt, dass die formalen Methoden nur unter Anwendung von spezifischen Rechnerwerkzeugen nutzbar sind. Obwohl die Leistungsfähigkeit der Rechentechnik in

den letzten Jahren stark gestiegen ist, gibt es bislang kein passendes Werkzeug, das die Anforderungen der formalen systemspezifikationsbasierten Sicherheitsanalyse der Bahnsysteme vollständig erfüllen würde.
Die Unzugänglichkeit eines passenden Werkzeuges führt dazu, dass die Beschreibung und Analyse von komplexeren Wirkungsketten gar nicht formalisiert wird. Dies betrifft insbesondere die Zusammenwirkung von mehreren technischen Systemen und die aus dem Betriebsprozess stammenden Einflüsse. Die Unmöglichkeit der genaueren Beschreibung des Eisenbahnbetriebsprozesses führte dazu, dass in den traditionellen Sicherheitsanalysen meistens die Vorgehensweise angewendet wurde, die auf der Beschreibung der Wirkungsketten lediglich innerhalb der technischen Systemimplementierung basieren. Um die durch die Norm 50126 geforderte Aussage über die Akzeptanz des betrieblichen Risikos zu beweisen, wird dabei auf das akzeptierbare Risiko eines funktional vergleichbaren technischen Systems hingewiesen, das sich bereits im Betrieb befindet und daher sein Risiko als akzeptiert gilt (entspricht dem Akzeptanzkriterium GAMAB, bzw. GAME, s. Kapitel 2.1.2). Eine solche Vorgehensweise nutzt nicht die Möglichkeit der Risikokompensation durch mehrere Systeme, die durch die risikobasierte Definition der Sicherheit seitens der Norm gegeben wird. Darüber hinaus kann dieses Vorgehen für die Einführung neuartiger Betriebs- und Systemkonzepte hinderlich sein, da die Methode grundsätzlich nur unter Existenz eines funktional und betrieblich vergleichbaren Systems anwendbar ist. Die durch die europäische Sicherheitsrichtlinie angekündigte Festlegung der gemeinsamen Sicherheitsziele (CST) verschiedener Personengruppen (bis 2008) wird jedoch in Zukunft die quantitative Auswertung des betrieblichen Risikos verlangen.

1.3 Ziel dieser Arbeit

Ziel dieser Arbeit ist zu zeigen, wie die Nutzung eines formalen Beschreibungsmittels die risikobasierte Sicherheitsanalyse methodisch unterstützen kann.
Als geeignete formale Notation wurden Petrinetze gewählt. Diese Wahl wurde einerseits durch einen ausgereiften mathematischen Hintergrund und breite Analysemöglichkeiten begründet, die bereits zu vielen praktischen Anwendungen geführt haben, andererseits durch deren Universalität. Diese Universalität der Verwendung hat den Vorteil einer großen Vielseitigkeit, stellt aber zugleich sehr hohe Anforderungen an die Genauigkeit der Definition der Anwendungsvorschrift dieses Beschreibungsmittels.
Das wichtigste Ziel ist es, die praktische Anwendung der Methode dem Leser soweit wie möglich nahe zu bringen, ohne auf die tiefen mathematischen Grundlagen der Theorie der Petrinetze und deren Analyseverfahren einzugehen. Neben der Darstellung des Nutzungspotentials der formalen Herangehensweise wurde darauf geachtet, den

Bezug zum traditionellen Vorgehen beizubehalten und den formalen Ansatz als seine mögliche Erweiterung mit erkennbarem Mehrwert zu sehen. Die parallele Anwendung der einzelnen Schritte des vorgestellten methodischen Vorgehens an den Beispielen aus

dem Eisenbahnbereich soll die allgemeingültigen Ausführungen mit praxisnaher Erklärung unterstützen.

1.4 Gliederung dieser Arbeit

Nach der Einleitung wird im Kapitel 2 die Aufgabe der risikobasierten Sicherheitsanalyse erläutert. Es wird das Risiko definiert und die bekannten Ansätze zur Risikoakzeptanz vorgestellt. Auf diesen Grundlagen wird das durch die Norm empfohlene Vorgehen bei der Sicherheitsanalyse beschrieben und seine möglichen Schwachstellen diskutiert. Die traditionellen Beschreibungsmittel der Sicherheitsanalyse werden kurz präsentiert. Als eine Alternative stellt Kapitel 3 anschließend einen modellbasierten Ansatz vor. Neben dem Vorgehen werden im Detail die Anforderungen an das zu diesem Zweck notwendige Beschreibungsmittel und seine Analysemöglichkeiten aufgestellt.
Kapitel 4 wird der gewählten Notation der Petrinetze und deren Analysemöglichkeiten aus der Sicht des Anwenders gewidmet. Gleichzeitig werden die Bezüge zwischen den traditionellen Beschreibungsmitteln der Sicherheitsanalyse und den Petrinetzen erläutert und deren Anwendungsmöglichkeiten verglichen.
Kapitel 5 stellt detailliert das methodische Vorgehen der Modellbildung einer modellbasierten Sicherheitsanalyse vor. Der Schwerpunkt liegt auf der Beschreibung einzelner Schritte des Modellaufbaus in Bezug auf die zugehörige Phase der Sicherheitsanalyse (Risiko- und Gefährdungsanalyse) im Rahmen des funktionalen und technischen Entwurfs eines Systems aus dem Eisenbahnbereich. Die einzelnen beschriebenen allgemeinen methodischen Schritte werden parallel an den Anwendungsbeispielen erläutert.
Kapitel 6 zeigt daraufhin das methodische Vorgehen bei der Analyse des erstellten Modells zum Zweck seiner Verifikation, Validation und zur Ermittlung der quantitativen funktionalen und implementierungsspezifischen Sicherheitsziele als Ergebnis modellbasierter Risiko-, bzw. Gefährdungsanalyse.
Kapitel 7 stellt als ein integriertes Beispiel die Sicherheitsanalyse eines Bahnübergangssicherungssystems nach dem vorgestellten methodischen Vorgehen vor.
Kapitel 8 schließt die Arbeit mit einer inhaltlichen Zusammenfassung und einem Ausblick in die Zukunft ab.

Kapitel 2

Sicherheitsanalyse im Eisenbahnwesen

In Gegensatz zu dem traditionellen absoluten Verständnis der Sicherheit basieren die moderne Ansätze der Sicherheitsbeurteilung technischer Systeme der Eisenbahn auf der Ermittlung des betrieblichen Risikos als relative Wahrscheinlichkeit.

2.1 Risikobemessung

2.1.1 Risikodefinition

Das Risiko wird in der genannten europäischen Norm EN 50126 als die *Wahrscheinlichkeit des Auftretens einer Gefahr, die einen Schaden verursacht, sowie der Schweregrad eines Schadens* definiert [EN50126 1996]. Diese Formulierung entspricht der gängigen Definition in der für das Risiko gilt [Kuhlmann 1981]:

$$Risiko = Schadensumfang \times Schadenseintrittswahrscheinlichkeit \tag{2.1}$$

In der gleichen Norm wird die Gefahr als *eine physikalische Situation* definiert, *die potentiell einen Schaden für den Menschen beinhaltet*. Daher ist zu erwarten, dass als Schadensumfang insbesondere der Tod von Menschen oder deren Verletzung anzunehmen ist.
Die risikobasierte Definition der Sicherheit in der geltenden Legislative des Eisenbahnwesens fordert von einem Bahnbetreiber bei der Einführung neuer Systeme die Sicherheitsanforderungen mittels der Auswertung des bestehenden betrieblichen Risikos zu bestimmen. Nach der Norm EN 50126 ist die dazu notwendige Risikoanalyse in die Sicherheitsplanung für den gesamten Lebenszyklus des Systems eingeordnet.

Zur Analyse des vorhandenen Risikos können zwei verschiedene Sichten angewendet werden:

- die Sicht des *kollektiven* Risikos, das der erwarteten Anzahl an Todesopfern innerhalb eines festgelegten Zeitraums aus dem Blickwinkel des Betreibers des Systems Eisenbahn bzw. der gesamten Gesellschaft entspricht oder
- die Sicht des *individuellen* Risikos, die das persönliche Risiko eines Individuums betrachtet, das dem Betrieb des Systems Eisenbahn ausgesetzt ist.

Das kollektive Risiko eines Systems kann z.B. als Anzahl der durch das System verursachten Toten pro Jahr angegeben werden. Um eine bessere Vergleichbarkeit zu erreichen, werden häufig leistungsbezogene Bezugswerte verwendet (z.B. Tote pro Fahrgastkilometer, Tote pro Zugkilometer) oder Größen bezogen auf bestimmte Systemmerkmale (z.B. Streckenkilometer, Anzahl der Bahnübergänge usw.).
Das individuelle Risiko wird meistens in Form von Toten pro Systembenutzer und Jahr angegeben. Dabei ist zu beachten, ob sich der betrachtete Zeitraum des Risikos auf die Verweilzeit im Gefahrenbereich oder auf einen beliebigen Teil des Lebenslaufs des Individuums bezieht. Ist $R_{\Delta t}$ das Individualrisiko während der Aufenthaltszeit eines Menschen im Gefahrenbereich und ist der relative Anteil dieser Aufenthaltszeit an dem umfassenden Abschnitt Δt seiner Lebenszeit durch σ gegeben, so ist der Anteil ΔR_{ind} des Risikos im betrachteten Gefahrenbereich am gesamten Risiko des Individuums unter realen Lebensbedingungen gegeben durch

$$\Delta R_{ind} = R_{\Delta t} \cdot \sigma \tag{2.2}$$

Sei N die Anzahl der Menschen im Betrachtungsbereich. Das globale Risiko R_{glob} steht dann mit dem individuellen in folgender Beziehung

$$R_{glob} = \Delta R_{ind} \cdot N \tag{2.3}$$

Um eine Einbeziehung der Verletzten in die Risikobewertung zu ermöglichen, wird durch die Norm EN 50 126 eine Umrechnung auf Tote empfohlen. Dabei entsprechen einem Toten 10 Schwerverletzte oder 100 Leichtverletzte, die jedoch von anderen auf monetäre Werte umgerechneten Verhältnissen abweicht [Rackwitz 2003]. Nach einer Analyse des vorhandenen Risikos ist es notwendig zu bewerten, wie groß das unzulässige Risiko für die Gesellschaft bzw. für den individuellen Systembenutzer ist.

2.1.2 Risikoakzeptanz

Abbildung 2.1 zeigt das allgemeine Vorgehen zur Bewältigung eines unzulässig großen betrieblichen Risikos. Das Vorgehen basiert auf der Bestimmung eines Restrisikos, das

das Maß für die notwendige Risikoreduktion durch die Funktionalität eines ELSS bildet. Dabei hängt die Größe des Restrisikos und des Sicherheitsfaktors von der Wahl des Akzeptanzkriteriums und von dem konkreten Anwendungsfall ab.

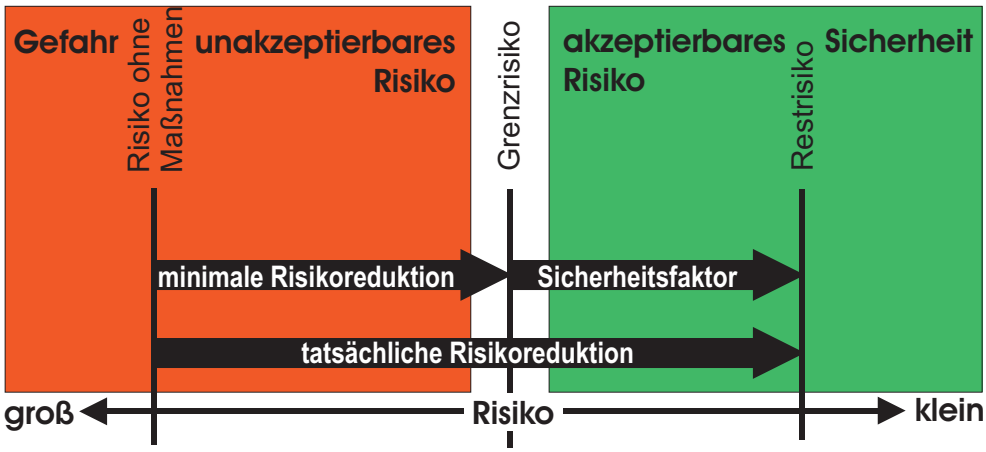

Abbildung 2.1: Allgemeine Aufgabe der Risikoreduktion

Als Basis der Entscheidung über die Risikoakzeptanz führt die Norm EN 50126 die Häufigkeit-Konsequenz-Matrix (s. Abbildung 2.2) ein. Dabei werden die Zeilen der Matrix mit Häufigkeiten der Gefahrenfälle und die Zeilen mit dem Schadenumfang (Risikostufen) attributiert. Den auf diese Weise erhaltenen qualitativen Risikokategorien werden entsprechende Maßnahmen zugeordnet, die aussagen, ob das jeweilige Risiko zulässig oder weiter zu reduzieren ist. Die Norm weist darauf hin, dass die Anzahl der Kategorien, deren quantitative Bewertung der Häufigkeiten anwendungspezifisch ist und deren passende Festlegung dem Eisenbahnunternehmen überlassen wird. Es wird dabei nur empfohlen, dass sich *die Akzeptanz der Risiken auf ein im Grundsatz anerkanntes Prinzip abstützen soll*, wobei die folgenden drei Prinzipien genannt und im Anhang detailliert beschrieben werden:

- ALARP (As Low As Reasonably Practicable) – unterscheidet drei verschiedene Zielgruppen der Individuen, die dem Risiko des Eisenbahnsystems ausgesetzt sind (Angestellter, Pendler, Anwohner). Für die Zielgruppen wird jeweils die obere Grenze des zulässigen Risiko (z.B. für einen Pendler darf das Risiko 1E-4 Tote pro Person und Jahr in keinem Fall überschritten werden) sowie die untere Grenze (das Risiko unter 1E-6 Tote pro Person und Jahr (Pendler) ist immer akzeptiert) definiert. Falls das resultierende Risiko zwischen den Grenzen liegt sind nur Maßnahmen zur Risikoreduktion zu ergreifen, die aus der Sicht der Wirtschaftlichkeit sinnvoll sind. In diesem Fall setzt das Kriterium also eine Kosten-Nutzen Analyse voraus.

Häufigkeit der Gefahrenfälle	Risikostufen			
häufig	intolerabel	intolerabel	intolerabel	unerwünscht
wahrscheinlich	intolerabel	intolerabel	unerwünscht	tolerierbar
gelegentlich	intolerabel	unerwünscht	unerwünscht	tolerierbar
selten	unerwünscht	unerwünscht	tolerierbar	vernachlässigb.
unwahrscheinlich	tolerierbar	tolerierbar	vernachlässigb.	vernachlässigb.
unvorstellbar	vernachlässigb.	vernachlässigb.	vernachlässigb.	vernachlässigb.
	katastrophal	*kritisch*	*marginal*	*unbedeutend*
	Gefahrenstufen			

Abbildung 2.2: Beispiel einer Risikoakzeptanzmatrix nach [EN50126 1996]

- GAMAB (Globalement Au Moins Aussi Bon) oder auch GAME (Globalement Au Moins Équivalent) – lässt sich sowohl aus der Sicht des individuellen als auch des kollektiven Risikos anwenden. Dem Kriterium liegt die Anforderung zugrunde, dass alle neuen spurgeführten Transportsysteme höchstens das gleiche Niveau des Globalrisikos aufweisen dürfen, wie vergleichbare bereits existierende Systeme. Es wird vorausgesetzt, dass das Risiko der bestehenden Systeme sich (z.B. anhand existierender Statistiken) bewerten lässt. Der Vergleich des Risikos eines bestehenden und eines neuen Systems ist nur möglich wenn auch die Leistungscharakteristiken und Betriebsbedingungen beider Systeme vergleichbar sind.

- MEM (Minimale Endogene Mortalität) – geht von der Voraussetzung aus, dass das absolute Gesamtrisiko der technischen Systeme, die auf ein Individuum wirken, höchstens den Wert minimaler menschlicher Sterblichkeit $2 \cdot 10^{-4}$ Tote pro Person und Jahr) betragen darf. Unter der Annahme, dass eine Person gleichzeitig bis zu 20 technischen Systemen ausgesetzt werden kann, ist das für das Gesamtsystem Eisenbahn (Fahrzeuge sowie Strecke) zulässige Risiko $1 \cdot 10^{-5}$ Tote pro Person und Jahr.

Neben den in der Norm erwähnten Ansätzen werden einige weitere Methoden zur Risikoakzeptanz und -bewertung im Eisenbahnwesen praktiziert (z.B. MGS – Mindestens Gleiche Sicherheit, NMAU – Nicht Mehr Als Unvermeidbar). Eine Alternative bietet auch die neuartige Sicherheitsklassifizierung der Systeme in Form der mittleren Verkürzung der menschlichen Lebensdauer [Schnieder et al. 2005]. Eine Kosten-Nutzen Analyse (z.B. unter Anwendung des ALARP Prinzips) kann auf Bewertung des „Life Quality Index“ basieren [Rackwitz 2003]. Dieser Wert stellt den Anteil des groben Inlandsprodukts, der zur Risikoreduktion zur Verfügung steht, in Bezug zu der mittleren

Lebenserwartung und der Arbeitszeit, die zum Verdienst eines mittleren Einkommens notwendig ist. Für hoch entwickelte westeuropäische Länder wird nach diesem Kriterium der Wert eines menschlichen Lebens mit 4 Millionen Euro geschätzt.
Obwohl viele veröffentlichte praktische Erfahrungen mit der Norm EN 50126 [Braband und Lennartz 1999, Stanley und Stutzbach 2006] die vergleichbasierten Ansätze der Risikoakzeptanz (z.B. GAME, MGS) bevorzugen, deutet die im Jahr 2004 herausgegebene Sicherheitsrichtlinie [2004/49/EC 2004] der Europäischen Kommission darauf hin, dass es zukünftig allgemeingültige Sicherheitsziele im Eisenbahnwesen in Form von zulässigen individuellen Risiken verschiedener beteiligter Personengruppen (Fahrgäste, Angestellte, Bahnübergangsnutzer usw.) geben wird. Mit Erarbeitung der Sicherheitsziele ist die vor kurzem gegründete Europäische Eisenbahnagentur ERA (European Railway Agency) beauftragt worden.
In der vorliegenden Arbeit, deren Schwerpunkt in der Vorstellung der Potentiale einer formalen Modellierung für die Sicherheitsanalyse liegt, wurde als Beispiel für die Risikoakzeptanz das Kriterium MEM herangezogen. Obwohl seine praktische Anwendung mit nicht geringer Weiterforschung und Normarbeit verbunden ist, ermöglicht dieses Kriterium das positive Potential der risikobasierten Sicherheitsphilosophie ausreichend darzustellen.

2.2 Risikofaktoren im System Eisenbahn

Das Risiko im Eisenbahnbetrieb wird durch das Potential von möglichen betrieblichen Ereignissen repräsentiert, die für die beteiligten Menschen eine Gefahr darstellen, d. h. sie können Tötung oder Verletzung eines menschlichen Individuums verursachen.
Abbildung 2.3 zeigt die Betrachtungsebenen der Sicherheitsanalyse eines allgemeinen ELSS in Form eines in Ebenen strukturierten und auf die wesentlichen Zustände (Elipsen) und Ereignisse (Balken) konzentrierten stochastischen Petrinetzmodells (s. Kapitel 4 mit dem Unterschied, dass die Initialmarkierung hier durch einen verstärkten Rand der Plätze dargestellt ist).
Die oberste Ebene bildet den eigentlichen Verkehrsprozess ab, in dem die unerwünschten Betriebssituationen (Unfälle) und der potentielle (Personen)schaden (Maß für die Sicherheitsbewertung) auftreten können. Einem Unfall geht immer eine Gefahrsituation voraus, in der durch eine externe Gefahrerkennung (inklusive Beinaheunfall) der Unfall noch vermieden werden kann. Andernfalls wird der sichere Verkehrsprozess nur noch durch die Unfallbergung wiederhergestellt.
Ein korrekter funktionaler Entwurf des ELSS soll dafür sorgen, dass beim sicheren Systembetrieb keine Gefahrsituationen im Verkehrsprozess vorkommen (außerhalb des tolerierbaren Restrisikos). Daher kann nur ein gefährlicher Systemfehler eine Ursache

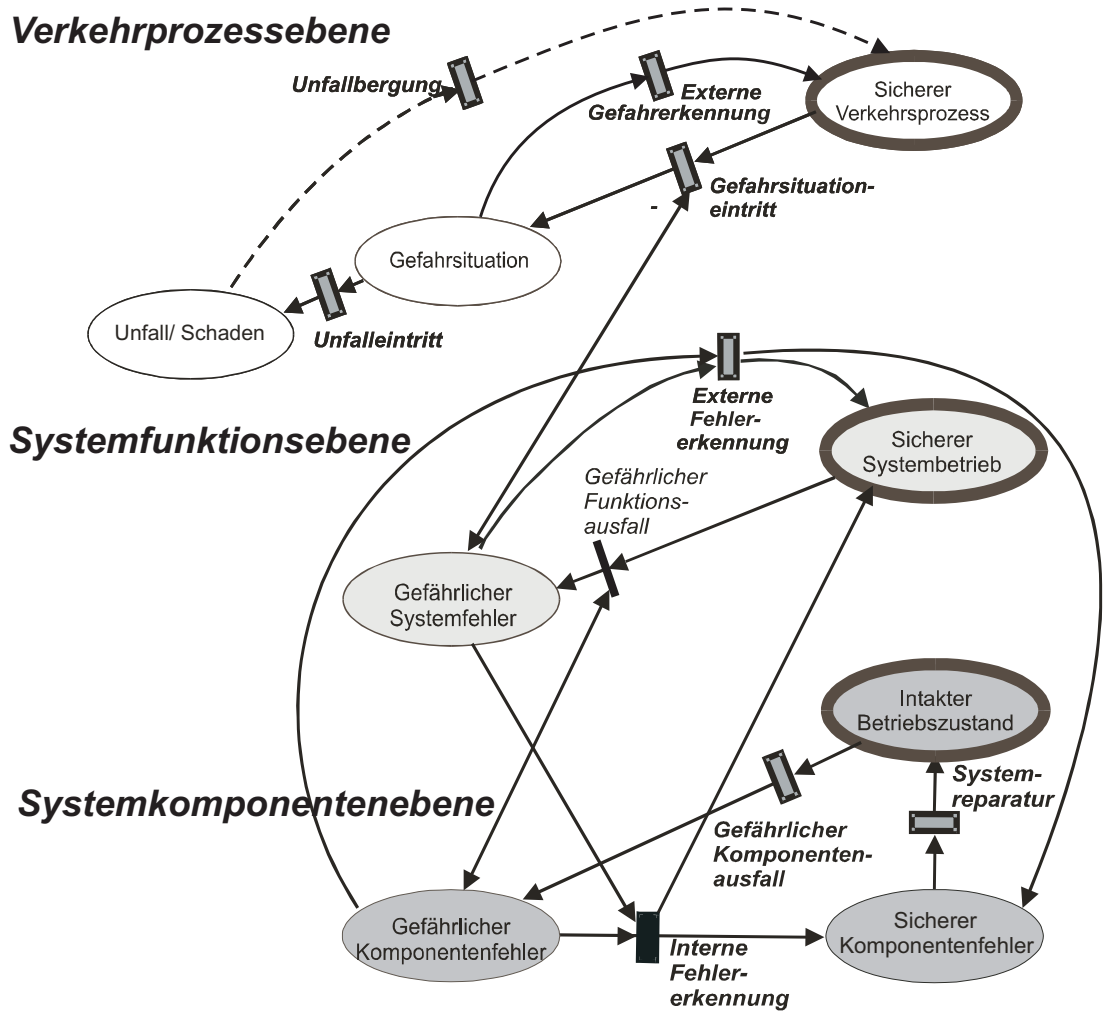

Abbildung 2.3: Betrachtungsebenen der Sicherheitsanalyse eines allgemeines Eisenbahnleit- und -sicherungssystems

des Gefahrensituationseintrittes sein, wie es im mittleren Teil der Abbildung 2.3 mit einer Doppelkante (Testkante) dargestellt ist. Eine andere externe Erkennung des gefährlichen Systemfehlers kann auch noch vor dem Eintritt der Gefahrsituation den sicheren Systembetrieb wieder herstellen.

Wie Abbildung 2.3 zeigt, hängt der Eintritt des gefährlichen Systemfehlers direkt von der Implementierung (Komponentenebene inklusive menschliche Ausführung) des ELSS ab. Die Modellierung des gefährlichen Funktionsausfalls ist daher eine kausale Folge eines gefährlichen Komponentenfehlers nach einem gefährlichen Komponentenausfall. Die technische Implementierung der Funktionen des ELSS kann auch Mechanismen einer internen Fehlererkennung vorsehen, die z.B. innerhalb eines deterministischen Intervalls das Erreichen eines sicheren Komponentenfehlers (sicheren Fehlzustandes des Systems) ermöglichen. Erst die Systemreparatur stellt den intakten Betriebszustand wieder her.

Tabelle 2.1 zeigt eine mögliche Konkretisierung des beschriebenen Modells, wobei als Beispiele der unerwünschten betrieblichen Ereignisse Kollision und Entgleisung verwendet wurden.

Betriebliches unerwünschtes Ereignis	Gefahrsituation	Gefährlicher Systemfehler	Gefährlicher Komponentenfehler
Zusammenprall	Straßenfahrzeug im Gefahrenraum und Zug in Annäherung	Versagen der BÜ Sicherung	Ausfall des Fahrzeug-erkennungssensors
Aufprall	Personen im Streckenbereich	Verletzung der Organisationsregeln	Menschliche Unaufmerksamkeit
Entgleisung	Freigegebene Fahrstrasse enthält Weiche in Zwischenlage	Versagen der Fahrwegsicherung	Gefährlicher Ausfall Endlagenmeldung
Zusammenstoß	Zwei Züge in einem Streckenabschnitt	Versagen der Fahrzeugsicherung	Versagen der der Geschwindigkeitsüber-wachung mit der Signalmissachtung

Tabelle 2.1: Beispiele unerwünschter betrieblicher Ereignisse und deren funktionale und technische Ursachen

2.3 Sicherheitsanalyse nach CENELEC

Abbildung 2.4 zeigt den Lebenszyklus eines Eisenbahnsystems mit den Phasen Entwurf, Herstellung und Betrieb nach der DIN EN 50126. Die Sicherheitsanforderungen an das Eisenbahnsystem werden einerseits in der Phase des Entwurfs, als Ergebnis der Risikoanalyse, andererseits in der Phase der Zuteilung der Systemanforderungen als komponentenspezifische Grenzwerte der Ausfallraten festgelegt. In beiden Phasen besteht die Aufgabe, eine stochastische Auswertung durchzuführen mit dem Ziel, die lokalen Eigenschaften des Systems (seiner Funktionen bzw. Komponenten) so festzulegen, dass die geforderten globalen Systemeigenschaften eingehalten werden.

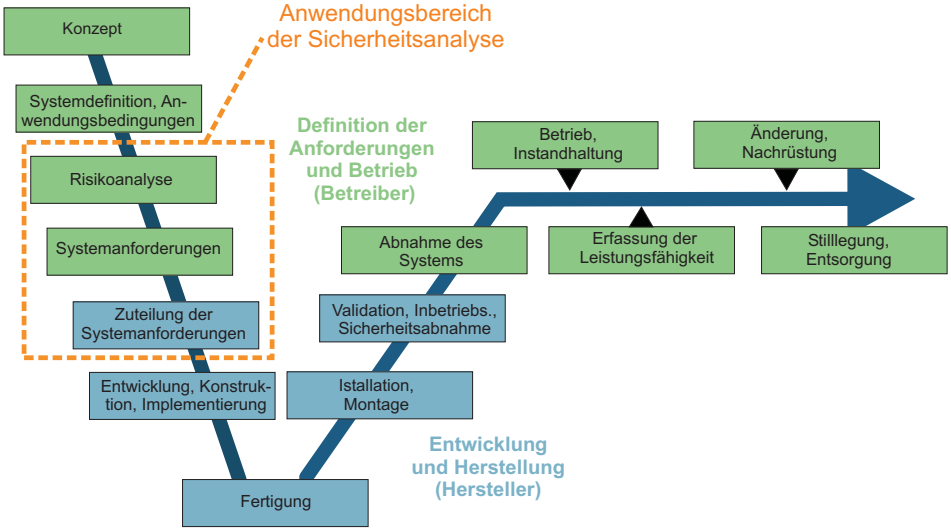

Abbildung 2.4: Integration der Sicherheitsanalyse in den durch die Norm EN 50126 vorgegebenen Lebenszyklus der Eisenbahnsysteme [Koch 2005]

In der Phase des Systementwurfs ergibt sich für den Systembetreiber die Notwendigkeit, die lokalen Sicherheitsanforderungen der einzelnen Systemfunktionen vorzuschreiben um das globale zulässige Risiko im Eisenbahnbetrieb (s. Unterkapitel 2.1.2) nicht zu überschreiten. Für den Systemhersteller sind diese Sicherheitsanforderungen an die Funktionen des Betreibers wiederum die globalen Ziele, die er durch richtige Festlegung der Anforderungen an die Systemkomponenten einhalten muss.
Dieses normativ vorgegebene Vorgehen ermöglicht, die Sicherheitsanforderungen genau an der notwendigen Risikoreduktion in dem Eisenbahnprozess auszurichten. Voraussetzung dafür ist eine ausreichende Genauigkeit der stochastischen Beschreibung, gegeben zwar einerseits durch die verfügbaren statistischen Eingangsdaten, andererseits aber durch die angewendete Beschreibungsmethode.

Das Vorgehen der Sicherheitsanalyse wird also in die Risiko- und die Gefährdungsanalyse (auch System- oder System-Hazard-Analyse genannt) unterteilt, Dieses Vorgehen wird im deutschsprachigen Raum graphisch in Form einer Sanduhr abgebildet und so genannt - ähnlich dargestellt in Abbildung 2.5. Die Schnittstelle zwischen der Risiko- und Gefährdungsanalyse bilden die funktionalen Sicherheitsziele in Form von tolerierbaren Häufigkeiten (mittleren Raten) der Gefährdungsauftritte (auch tolerierbare Hazardraten - *THr* - genannt).

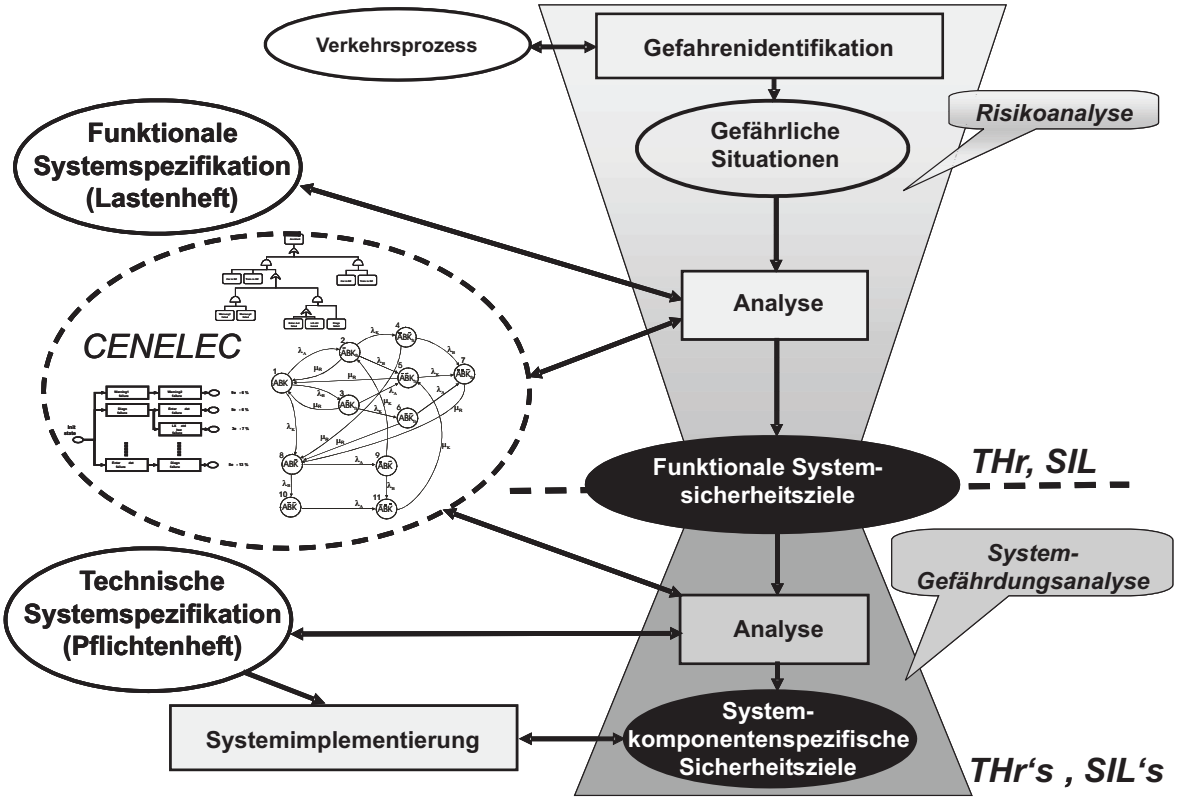

Abbildung 2.5: Hauptaufgaben der Sicherheitsanalyse

2.3.1 Risikoanalyse

Die Aufgabe der durch den Betreiber durchzuführenden Risikoanalyse ist, das beim Betrieb des ELSS auftretende Risiko zu quantifizieren. Dabei soll das Eisenbahnleitsystem nur aus funktionaler und rein betrieblicher Sicht betrachtet werden, ohne mögliche technische Realisierungen zu berücksichtigen.
Der erste Schritt der Risikoanalyse ist die Systemdefinition, in deren Rahmen die Funktionsanforderungen für das betreffende System festzulegen sind. Diese beinhalten den

zu steuernden Verkehrsprozess und alle betriebsbezogenen Systemparameter, die meistens in Form einer funktionalen Systemspezifikation gegeben sind.
Ein weiterer Schritt besteht darin, anhand der bekannten Interaktion zwischen dem ELSS und dem Verkehrsprozess die möglichen gefährlichen Situationen im Betrieb (Gefahren) zu identifizieren.
Im Rahmen einer darauf folgenden Gefahrenanalyse sind dann sowohl die Folgen der gefährlichen Situationen in Form des resultierenden Risikos (z.B. Individuelles Risiko als Anzahl der Toten pro Person und Jahr) zu quantifizieren, als auch die im Sinne funktionaler Systemspezifikation möglichen systembezogenen Ursachen (Gefährdungen) zu identifizieren.
Ergebnis der Risikoanalyse sind dann die systemfunktionsbezogenen tolerierbaren Gefährdungsraten (THr) als quantitative funktionale Sicherheitsziele, die anhand der bekannten Beziehung zum resultierenden betrieblichen Risiko und unter Anwendung eines geeigneten Risikoakzeptanzkriteriums (z.B. MEM, GAMAB, ALARP) [EN50126 1996] abzuleiten sind.

2.3.2 Gefährdungsanalyse

Anhand der Ergebnisse der Risikoanalyse ist die Aufgabe der durch den Systemhersteller durchzuführenden Gefährdungsanalyse, die ermittelten funktionalen Sicherheitsziele auf die einzelnen Komponenten der technischen Systemimplementierung zu verteilen.
Daher ist es der erste Schritt der Gefährdungsanalyse, auf der Basis der technischen Systemspezifikation für jede Gefährdung die entsprechenden Ursachen in der Komponentenverlässlichkeit durch Analyse herauszufinden. Anhand der Kenntnis der Verlässlichkeitsparameter der Komponente ist die Aufgabe des Herstellers, eine geeignete Systemarchitektur zu entwerfen, damit die gesetzten funktionalen Sicherheitsziele eingehalten werden. Diese Aufgabe umfasst insbesondere die Integration zusätzlicher technischer und organisatorischer Maßnahmen (wie z.B. Redundanz, Diagnostik, Wartungsintervalle usw.) mit dem Ziel durch Erhöhung der Verlässlichkeitseigenschaften der technischen Lösung die Sicherheitsziele zu erreichen.
Ergebnis der Gefährdungsanalyse ist eine konkrete technische Systemspezifikation mit systemkomponentenspezifischen Sicherheitszielen in Form von tolerierbaren Ausfallraten inklusive aller Anforderungen an die Zuverlässigkeit und Instandhaltbarkeit.

2.3.3 Traditionelle Methoden

Als Mangel der heutigen CENELEC-Normen wird oft bezeichnet [Braband und Lennartz 2003, Knewitz 2005], dass sie zwar eine sehr umfassende Orientierung darüber bieten, wie bestimmte Sicherheitsanforderungen erreicht werden können, jedoch das

Verfahren und die Regeln zur Ableitung von Sicherheitsanforderungen für Systemkomponenten aus den Sicherheitszielen oder dem zulässigen betrieblichen Risiko nicht genau definiert sind. Für diese Aufgaben wird im Anhang der Norm 50 129 eine Reihe von Methoden wie FMEA (Failure Mode and Effect Analysis), FMECA (Failure Mode and Effect Criticality Analysis), ETA (Event Tree Analysis), FTA (Fault Tree Analysis), Markovketten oder RBD (Reliability Block Diagrams) empfohlen, die sowohl im Rahmen der Risikoanalyse als auch der Gefährdungsanalyse Einsatz finden können (s. Abbildung 2.5).
Tabelle 2.2 zeigt die möglichen Einsatzbereiche der genannten Methoden im Rahmen der einzelnen Schritte der Sicherheitsanalyse. Die entsprechende Bewertung zeigt den Grad ihrer Eignung für Aufgaben, die im Rahmen einer Sicherheitsanalyse durchzuführen sind.

Methode	Gefährdungs-identifikation	Risikoanalyse	Gefährdungs-analyse	Sicherheits-nachweis
ETA	Nicht anwendbar	Anwendbar	Möglich	
FMECA	Anwendbar	Anwendbar nur für serielle Systeme ohne Redundanz	Anwendbar für serielle Systeme ohne Redundanz	
FTA	Nicht anwendbar	Möglich	Anwendbar	
HAZOP	Anwendbar	Nicht anwendbar	Nicht anwendbar	
Markovketten	Nicht anwendbar	Anwendbar	Anwendbar	
RBD	Nicht anwendbar	Nicht anwendbar	Anwendbar für nicht reparierbare Systeme	
CCF-Analyse	Nicht anwendbar	Unterstützend	Unterstützend	

Tabelle 2.2: Einsatzbereiche der Methoden im Rahmen der Sicherheitsanalyse nach [Braband 2005]

2.3.4 Traditionelle Beschreibungsmittel

Die Methoden der Sicherheitsanalyse basieren auf Beschreibungsmitteln mit sehr unterschiedlichem Formalisierungsgrad. Einige wie z.B. HAZOP (Hazard Operation Analysis) [Fenelon et al. 1995], FMEA (Failure Mode and Effect Analysis) [Gralla und Heinz 1998] oder FMECA (Failure Mode and Effect Criticality Analysis) [Reifer 1979] basieren auf einer Textbeschreibung der kausalen Zusammenhänge zwischen Gefahrsituationen, Gefährdungen und deren technischen Ursachen in tabellarischer Form. Andere Methoden wie ETA (Event Tree Analysis) oder FTA (Fault Tree Analysis) [Vesely et al. 1981] [IEC 61025 2003] beschränken sich auf graphische Darstellungen von kausalen Folgen (ETA) oder Beziehungen (FTA), die mit Auftrittswahrscheinlichkeiten parametriert werden. Dadurch ist es möglich, die Wahrscheinlichkeit eines Top-Ereignisses auszuwerten. Ein Beispiel einer bahnspezifischen Anwendung zeigt Abbildung 2.6.

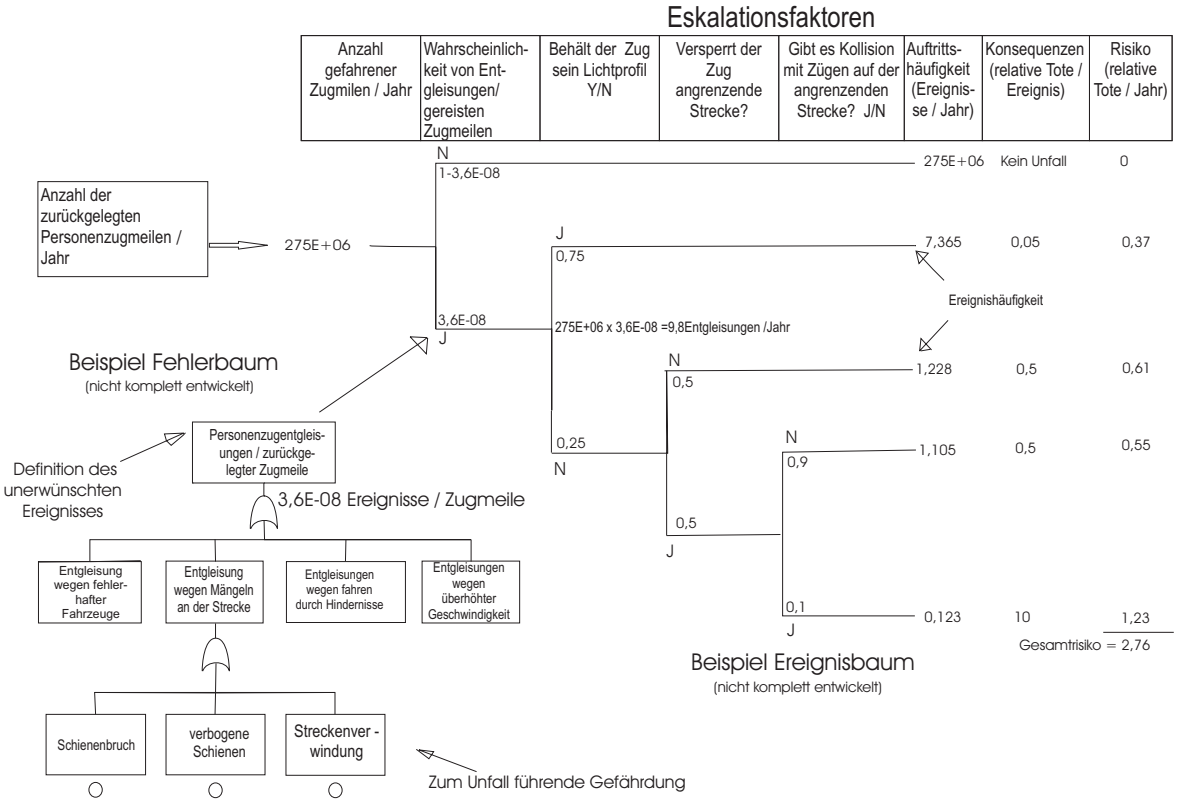

Abbildung 2.6: Beispiel einer Fehlerbaum- und Ereignisbaumanalyse in Bahnbereich nach [Bearfield 2005]

Zur Beschreibung von stochastischen temporalen Folgen werden damit ausschließlich die Markovketten verwendet [IEC 61165 2005], deren Beschränkung auf die Exponentialverteilung und darauf basierende Gedächtnislosigkeit des beschriebenen Verhaltens mit vielen Vereinfachungen einhergeht. Darüber hinaus verhindert die Modellierung von rein globalen Systemzuständen ihre praktische Anwendbarkeit für komplexere Systeme, insbesondere für ihre Beschreibung entsprechend den iterativen Änderungen der Systemarchitektur während der Entwurfsphase. Ein Beispiel zeigt Abbildung 2.7.

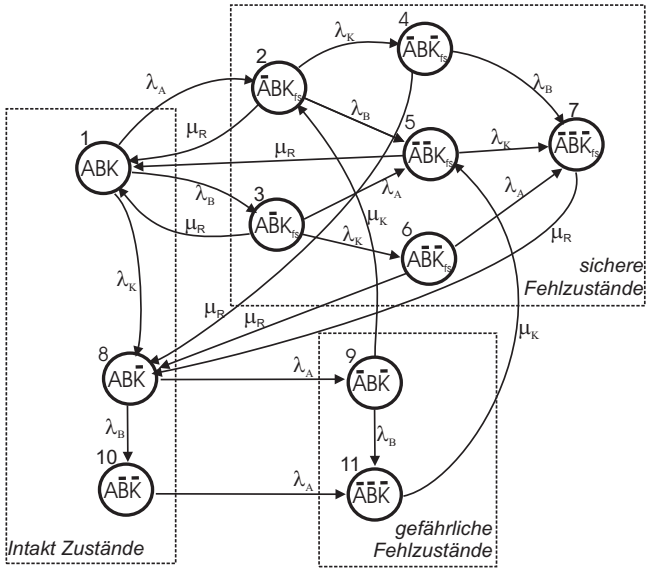

Abbildung 2.7: Beispiel einer Markovkette

Zum Entwurf von Systemarchitekturen werden häufig die Zuverlässigkeits-Block- Diagramme (RBD - Reliability Block Diagramms) angewendet. Sie ermöglichen, die verschiedensten Arten der Redundanz und Komponentenkonfigurationen zu beschreiben und hinsichtlich der Verlässlichkeit auszuwerten. Da es sich nur um eine reine Verlässlichkeitsbeschreibung handelt, können die Aspekte des temporalen Regelverhaltens des Systems (z.B. Wartung- und Diagnostikintervalle) nicht direkt integriert werden. Auch eine Beschreibung des Verkehrsprozesses oder der Systemfunktionalität ist nicht möglich.

Tabelle 2.2 stellt eine Übersicht der in der Praxis meistens angewendeten Methoden im Kontext von Sicherheitsanalysen dar, die auf der Verwendung von konventionellen Beschreibungsmitteln basieren. Die Tabelle zeigt deutlich, dass die Einsatzbereiche der einzelnen Methoden recht unterschiedlich sind und daher im Rahmen einer Sicherheitsanalyse für verschiedene Aufgaben unterschiedliche Beschreibungen (Modelle) des Systems notwendig sind. Wie aus der Tabelle ersichtlich ist, sind diese Methoden nicht

durchgängig einsetzbar und deren Beschreibungsmittel meistens nicht systematisch ineinander überführbar. Eine formale Verifikation oder eine Art der Unterstützung der Modellvalidation sind hier in der Regel ausgeschlossen.

2.4 Zusammenfassung

Anhand der existierenden Legislative und unter Berücksichtigung vieler Erfahrungsberichte kann gesagt werden, dass die Sicherheitsanalyse im Eisenbahnwesen heutzutage mehr oder weniger auf einer informalen oder semi-formalen Grundlage durchgeführt wird. Die Forderung die Sicherheitsziele auf der Basis des betrieblichen Risikos zu definieren ist bei zunehmender Komplexität der zu analysierenden Systeme stark fehleranfällig. Eine holistische formale Unterstützung des Vorgehens bei der Sicherheitsanalyse scheint ein großes praktisches Nutzungspotenzial zu bieten.

Kapitel 3

Modellbasierte Sicherheitsanalyse - PROFUND-Konzept

Eine Alternative zur Anwendung der genannten traditionellen Methoden bietet ein modellbasierter Ansatz. Dieser basiert auf der Verwendung von formalen Beschreibungen, deren Einsatzberechtigung in der Softwareentwicklung oder Systemspezifikation in der letzten Zeit mehrmals erfolgreich und auch praktisch bewiesen wurde. Auch im Einsatzbereich der Sicherheitsanalyse sind immer öfter Arbeiten zu finden, die versuchen dieses Vorgehen formal zu unterstützen. Als Beispiele seien hier die Arbeiten [Hansen 1996] [Montigel 1996] [Bitsch et al. 2004] [Klose 2003] [Arabestani 2005] oder [Ortmeier 2005] genannt, deren Anwendungsgebiete auch das Eisenbahnwesen umfasst. Diesen aus dem Informatikbereich stammenden Ansätzen ist gemeinsam, dass sie sich im wesentlichem darauf konzentriert haben, eine formale Systemspezifikation durch formal spezifizierte Sicherheitsanforderungen zu validieren. Eine Ableitung von quantitativen Sicherheitszielen auf der Basis des betrieblichen Risikos stand nicht im Anwendungsfokus dieser Ansätze.

Andere Arbeiten haben das Ziel, die meistens semi-formalen traditionellen Methoden der Sicherheitsanalyse durch bestimmte Erweiterungen zu formalisieren. Meistens wurden diese Ansätze auf die formale Fehlerbaumanalyse (FTA) erfolgreich angewendet [Trivedi et al. 1993, Buchacker 2000] wobei es auch darum ging, den rein statischen konventionellen Ansatz mit der Dynamik der relevanten Ereignisse zu erweitern [Thums 2004,Kaiser und Gramlich 2004] und so das Einsatzgebiet der Methode zu erweitern.

3.1 Ansatz

Um die Sicherheitsanforderungen für die Systemfunktionen sowie Systemkomponenten im Sinne der genannten Normen definieren und validieren zu können, ist es notwendig die Beziehung zwischen dem Auftritt unerwünschter betrieblichen Ereignisse (Unfälle) und dem funktionalen bzw. komponentenspezifischen Ausfallpotenzial (Verlässlichkeit) zu beschreiben. Abbildung 2.3 stellt auch die in einer Sicherheitsanalyse integrierten Beschreibungsobjekte dar, nämlich:

- den Verkehrsprozess, mit seinem Regel- und Gefahrablauf inklusive möglicher Unfälle,
- die Systemfunktionalität mit ihrem Regel- und Ausfallverhalten sowie
- die Systemimplementierung mit Regel- und Ausfallverhalten der Implementierungskomponenten.

Mit anderen Worten, die notwendige Modellierung richtet sich auf die Funktion und das stochastisch-deterministische Verhalten des Verkehrsprozesses, das deterministische Verhalten der korrekten Systemfunktionalität bzw. -implementierung sowie das stochastische Verhalten der Funktions- bzw. Implementierungsverlässlichkeit. Die integrierte Betrachtung des Prozesses (**PRO**cess), der Funktionalität (**FUN**ctionality) und Verlässlichkeit (**D**ependability) bildet die Basis des in dieser Arbeit zu Grunde gelegten *PROFUND*-Ansatzes. Abbildung 3.1 zeigt die relevanten Bereiche der Beschreibung für die Zwecke modellbasierter Sicherheitsanalyse im Sinne dieses Ansatzes.

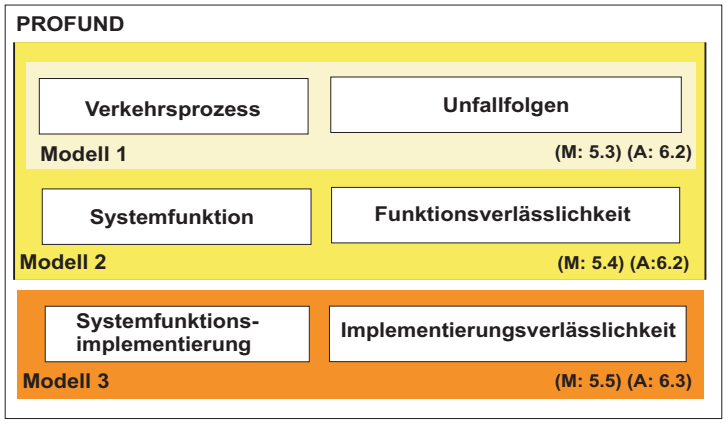

Abbildung 3.1: Die relevanten Bereiche der Beschreibung des *PROFUND*-Ansatzes mit dem Hinweis auf das zugehörige Unterkapitel dieser Arbeit mit entsprechender Erläuterung der Modellbildung (M) und -analyse (A)

Der *PROFUND*-Ansatz dient dazu, alle Aufgaben der Sicherheitsanalyse mit einer formalen Beschreibung durchgängig zu unterstützen. Er basiert auf einem Modell, das im Rahmen der Sicherheitsanalyse schrittweise aufgebaut wird, wobei es jederzeit zu quantitativen Auswertungen herangezogen werden kann. Abbildung 3.2 deutet dieses Vorgehen graphisch an.

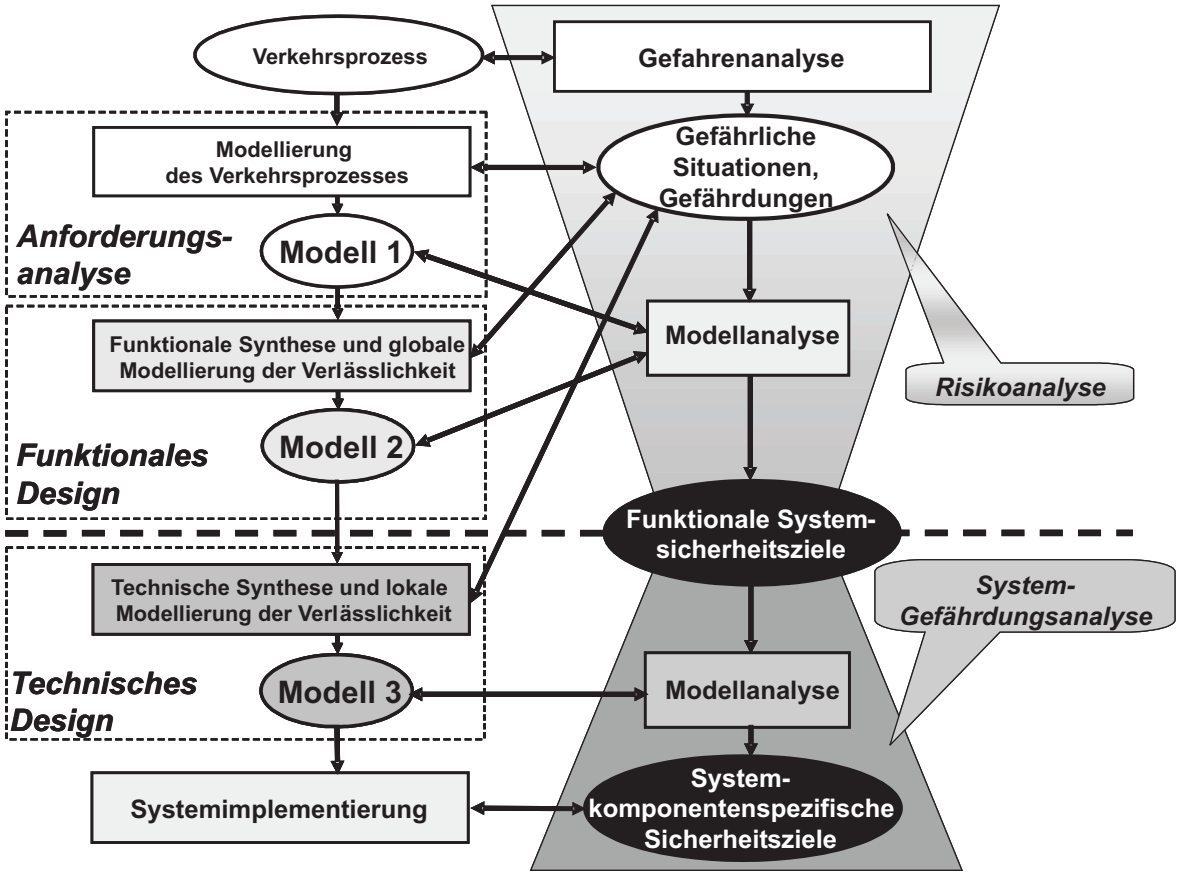

Abbildung 3.2: Modellbasierte Sicherheitsanalyse nach dem *PROFUND*-Ansatz

Entsprechend den in Abbildung 2.3 genannten Betrachtungsebenen wird im ersten Schritt auf der Basis des bekannten durch den ELSS zu steuernden Verkehrsprozesses (im Sinne der definierten Systemgrenzen) und nach durchgeführter Identifikation der Gefahren und deren potentiellen Folgen ein Modell des Betriebsprozesses aufgebaut (*Modell 1*). Dieses beschreibt nicht nur den Eisenbahnbetrieb mit seinen möglichen gefährlichen Situationen, sondern auch alle ihre potentiellen kausalen Folgen. Schon die Analyse dieses Modells kann zur Evaluation des betrieblichen Risikos verwendet werden. Da aber die Funktionalität des ELSS selbst nicht integriert wurde, sagen die Ergebnisse nur etwas über das hypothetische Betriebsrisiko eines ungesteu-

erten Eisenbahnverkehrs aus. Dennoch können sie unter Anwendung eines geeigneten Risikoakzeptanzkriteriums zur Quantifizierung der Anforderungen an die durch das ELSS notwendige Risikoreduktion verwendet werden. Durch Bildung des Modells des Verkehrsprozesses wird eine Vergleichsgrundlage für Einflüsse unterschiedlicher funktionaler oder technischer Spezifikationen des ELSS formal festgelegt.
Der nächste Schritt beinhaltet die Beschreibung der für die Sicherheitsanalyse relevanten Funktionalität des ELSS (im Sinne der Systemdefinition bzw. funktionalen Systemspezifikation). Aufgrund der eindeutigen Trennung zwischen dem Verkehrsprozess und der Systemfunktionalität kann anhand der identifizierten funktionalen Gefährdungen aus der Gefahrenanalyse die Beschreibung auch um das potentielle funktionale Verlässlichkeitsverhalten erweitert werden. Die Verbindung eines solches Modells mit dem Modell des Verkehrsprozesses (*Modell 2*) ermöglicht, anhand des bekannten tolerierbaren betrieblichen Risikos die funktionalen Systemsicherheitsziele in der Form von tolerierbaren Gefährdungsraten oder SILs der Funktionen auszuwerten. Diese bilden das Ergebnis der Risikoanalyse.
Die grundlegende technische Spezifikation des ELSS und die im Rahmen der Gefahrenanalyse identifizierten technischen Gefährdungen bilden die Basis zur Beschreibung der beabsichtigten technischen Implementierung und ihres Verlässlichkeitsverhaltens (*Modell 3*). Ein solches Modell kann durch Berücksichtigung der funktionalen Systemsicherheitsziele oder durch eine direkte Kopplung mit dem Modell 2 (Verkehrsprozess und Systemfunktionalität) zur Ermittlung von systemkomponentenspezifischen Sicherheitszielen in Form von tolerierbaren Ausfallraten verwendet werden (Ergebnis der Gefährdungsanalyse). Sind diese Ziele technisch nicht erreichbar, ist eine (auch iterative) Erweiterung der grundlegenden technischen Spezifikation um weitere Maßnahmen (wie Überwachung, Redundanz, usw.) zur Steigerung der Verlässlichkeit vorzunehmen. Werden die funktionalen Sicherheitsziele erreicht, kann die resultierende technische Spezifikation mit Angabe der systemkomponentenspezifischen Sicherheitsziele zur Implementierung des ELSS verwendet werden.

3.2 Anforderungen an die modellbasierte Sicherheitsanalyse

Um den vorgestellten Ansatz als Methode praktisch anwenden zu können ist es notwendig ein geeignetes Beschreibungsmittel und ein Werkzeug zur Verfügung zu haben [Schnieder 1999b]. Die formalen Techniken, deren Einsatz auch durch die Normen (z.B. EN 50129) nachdrücklich empfohlen wird, bieten dazu gute Voraussetzungen. Während das Beschreibungsmittel zur Notation der Sachverhalte dient, ist die Aufgabe einer Methode, die Regeln des Vorgehens zur Lösung einer Aufgabe zu de-

finieren. Eine Methode, die die Vorgehensweise unter Benutzung eines konkreten Beschreibungsmittels definiert, kann als eine Formale Technik bezeichnet werden [Einer 2003]. Eine praktische Anwendung einer Formalen Technik ist meistens nur durch ein Werkzeug möglich, heutzutage meistens durch ein Rechensystem (Hardware/Software) realisiert [Meyer zu Hörste 2003].
Das Ziel der allgemein beschriebenen Bildung des Modells ist seine quantitative Analyse, die die gesuchten quantitativen Ergebnisse wie Unfallraten, Auftrittswahrscheinlichkeiten gefährlicher Zustände, tolerierbaren Gefährdungsraten usw. ermitteln soll. Um aber eine bestimmte Überzeugung von der Plausibilität dieser Ergebnisse gewinnen zu können, ist es notwendig eine qualitative Analyse des Modells mit dem Ziel der Verifikation und Validation des Modells durchführen zu können.
Typischer Weise haben Ergebnisse der qualitativen Analyse binären Charakter, z.B. Erreichbarkeit eines bestimmten unerwünschten Zustandes, Geltung einer Modelleigenschaft oder einer Sicherheitsanforderung usw., oder sie sind von enumerativer Natur, z.B. Anzahl der Betriebszustände in einer Gefahrsituation, mögliche Pfade von einem Regelzustand zu einem Unfallzustand usw. Diese Art der Ergebnisse ermöglicht, das modellierte Verhalten mit den Ergebnissen der Gefahrenanalyse zu vergleichen und dadurch noch vor der quantitativen Analyse das Modell auf seine Korrektheit zu überprüfen (s. Kapitel 6).
Aus der geforderten Durchgängigkeit der Beschreibung resultiert eine Vielzahl von Anforderungen an das zu verwendende Beschreibungsmittel und an seine Analysemöglichkeiten.

3.2.1 Anforderungen an das Beschreibungsmittel

Die Anforderungen an das Beschreibungsmittel richten sich einerseits nach der Art des Systemverhaltens, das zu modellieren ist. Die *PROFUND*-Methode setzt voraus, deterministisch und stochastisch temporale Sachverhalte beschreiben zu können. Diese können durch konstante Zeitparameter oder stochastische Verteilungen oder Auftrittswahrscheinlichkeiten definiert werden. Es muss möglich sein für die im Modell beschriebenen Ereignisse Auftrittsbedingungen eindeutig zu definieren zu können.
Da *PROFUND* zugleich eine Top-Down Vorgehensweise vorschreibt (von Unfällen über Betrieb, Funktionalität und Verlässlichkeit zu den Gefährdungen) spielt in dem Modell die Beschreibung der kausalen (logischen) Beziehungen z.B. zwischen lokalen (Gefährdungen) und globalen (gefährliche Situationen, Unfälle usw.) Systemzuständen eine wichtige Rolle.
Die Top-Down Vorgehensweise stellt Anforderungen an die Ergonomie des Beschreibungsmittels. Dazu gehören hauptsächlich die Möglichkeiten der Hierarchisierung und der Modularisierung des Modells. Durch Bildung von kompositionalen Modellen soll es

ermöglicht werden, generische oder vorgefertigte Teilmodelle aus Bibliotheken zusammenzukoppeln und auf dieser Basis dem Anwender die Modellbildung zu erleichtern.

3.2.2 Anforderungen an die Analysemöglichkeiten

Die qualitative Analyse fordert eine Unterstützung bei der Untersuchung des erreichbaren Zustandsraumes des modellierten Systems. Anhand der unerwünschten betrieblichen Zustände muss es möglich sein, zur Validation des Modells die entsprechenden gefährlichen betrieblichen Situationen oder funktionale bzw. komponentenspezifische Gefährdungen zu identifizieren. Ebenso ist es von Interesse bestimmte Modelleigenschaften, die z.B. den Sicherheitsanforderungen an das modellierte System entsprechen, im Modell automatisch überprüfen zu können.
Durch die quantitative Analyse soll ermöglicht werden, die Wahrscheinlichkeit der unerwünschten oder gefährlichen Systemzustände bzw. die mittleren Häufigkeiten der entsprechenden relevanten Ereignisse sowohl in Bezug auf beliebige Zeitpunkte der Betriebsdauer des technischen Systems als auch in seinem eingeschwungenen Zustand zu bewerten (stationäre und transiente Analyse). Als Eingangsgrößen sind die statistischen Eigenschaften und Parameter des Betriebsprozesses sowie unterschiedliche stochastische Charakteristiken des Verlässlichkeitsverhaltens von funktionalen Ressourcen, technischen Systemkomponenten und Instandhaltungsprozessen heranzuziehen.

3.2.3 Anforderungen an die Toolunterstützung

Eine geeignete Toolunterstützung gehört zu den grunsätzlichen Anforderungen zur praktischen methodischen Anwendung des *PROFUND*-Ansatzes. Dabei handelt es sich insbesondere um Gewährleistung eines einfachen Wechsels zwischen der Modellbildung und der Modellanalyse, die während des beschriebenen methodischen Vorgehens mehrmals zum Einsatz kommen.
Der zur Modellbildung vorgesehene Editor soll eine handhabbare Ausnutzung des Beschreibungsmittels ermöglichen. Hierzu gehört auch eine Unterstützung bei der Beschreibung des stochastischen Verhaltens durch einen "Verteilungseditor" und die Möglichkeit der Eingabe von Daten aus Statistiken oder statistischen Messungen.
Im Weiteren sollen alle genannten Anforderungen an das Beschreibungsmittel wie Hierarchisierung und Modularität geeignet erfüllt werden. Ein wichtiger Aspekt dabei ist die Möglichkeit einfacher Änderung der Modulgrenzen oder der Hierarchieebenen durch Subnetz- und Supernetzbildung. Eine Modellbibliothek mit häufigst genutzten Modellbausteinen und einfacher Möglichkeit der Erweiterung soll die Ansprüche an die Erfahrung des Modellierers in akzeptierbaren Grenzen halten.

3.3 Zusammenfassung

Ein grundlegender Aspekt des vorgestellten *PROFUND*-Ansatzes ist, im Rahmen der Sicherheitsanalyse die Bereiche des Verkehrsprozesses, System- und Implementierungsfunktionalität sowie Funktions- bzw. Implementierungsverlässlichkeit zu integrieren. Ziel ist, den bereits etablierten Prozess der Sicherheitsanalyse mit einer formalen Basis zu unterzustützen, die ermöglichen würde, einerseits die Konsistenz der einzelnen Schritte zu gewährleisten und anderseits eine holistische quantitative Analyse zu ermöglichen, ohne vom Anwender hohe mathematische Kenntnisse zu verlangen. Tabelle 3.1 ordnet Lösungen zu den methodische Anforderungen des *PROFUND*-Ansatzes mit Referenz auf entsprechende Kapitel bzw. Unterkapitel dieser Arbeit, in denen detaillierte Beschreibungen gefunden werden können.

	Anforderungen	**Ansatz/Lösung**	**Referenz Erklärung**	**Referenz Beispiel**
Beschreibungsmittel	Stochastisches Verhalten	Exponentielle / allgemeine stochastische Transitionen	4.1.2	Kap. 5, 7.3.1, 7.5.1, 7.6.1
	Deterministisches Verhalten	Deterministische Transitionen		Kap. 5, 7.3.1, 7.4.1, 7.6.1
	Kausale Beziehungen	Kausale Transitionen		Kap. 5, 7.3.1, 7.4.1, 7.5.1, 7.6.1
	Bezug lokaler und globaler Zustände	Bildung der Superknoten		5.5.2, 7.6.1
Modellierung	Hierarchie	Bildung eines Unternetzes, einer Instanz	4.1.2	Kap. 5, 7.3.1, 7.4.1, 7.5.1, 7.6.1
	Modularität	Verbindung der Modelle nur durch Abfragekannten und Inhibitoren		Kap. 5, 7.3.1, 7.4.1, 7.5.1, 7.6.1
Qualitative Analyse	Top-Down	Graph Mengen globaler Zustände	4.1.3	6.2.1, 6.2.3, 7.3.2, 7.4.2, 7.5.2
		Unfallbaum		6.2.1, 6.2.3, 7.5.2
	Botton-Up	Rückwertsanalyse des Erreichbarkeitsgraphen		6.2.1, 7.3.2
	Verifikation der Modelleigenschaften	Invariantenanalyse		6.2.3
Quantitative Analyse	Auswertung der Raten, Auftrittswahrscheinlichkeiten	Analytische / Simulative Lösung	4.1.3	Kap. 6, 7.3.2, 7.4.2, 7.5.2, 7.6.2

Tabelle 3.1: Methodische Anforderungen und Lösungen des *PROFUND*-Ansatzes

Kapitel 4

PROFUND-Beschreibungsmittel

Als geeignetes Beschreibungsmittel zur Anwendung durch die *PROFUND*-Methode wurden in dieser Arbeit Petrinetze gewählt. Im Hinblick auf die im vorherigen Kapitel gestellten Anforderungen bieten Petrinetze - konkreter ihre stochastische Erweiterung, einen Formalismus, der Beschreibungen aller genannten Sachverhalte ermöglicht. Der präzise mathematische Hintergrund der Petrinetze erlaubt auch, die hohen Anforderungen an die notwendigen Analysemöglichkeiten zu erfüllen.

4.1 Petrinetze

4.1.1 Petrinetze im Eisenbahnwesen

Neben den anderen Bereichen der Ingenieurswissenschaften wurde das Thema "Modellierung, Analyse und Simulation der Bahnsysteme mit formaler Beschreibung der Petrinetze" bereits in mehreren Forschungsprojekten der Industrie und der Deutschen Forschungsgemeinschaft (DFG) behandelt. Zu erwähnen sind die Betriebsleittechnik für Transrapid [Schnieder 1996], SatZB Satellitengestütztes Eisenbahnleitsystem für Nebenbahnen [Meyer zu Hörste et al. 2000], Risikoanalyse der Pilotstrecke SBB von Mattstetten nach Rothrist sowie die Modellierung operationaler Prozesse der Eisenbahnsicherung [Einer 2003] im Rahmen des DFG-Schwerpunktprogramms Integration von Techniken der Softwarespezifikation für ingenieurwissenschaftliche Anwendungen. Im Rahmen der Arbeiten von [Decknatel 2001] wurde ein formales Beschreibungsmittel (Höhere hybride Petrinetze) für hybride Systeme entwickelt und für gemischt kontinuierlich-diskrete Modellierungen von Verkehrsprozessen der Bahnsysteme praktisch angewendet. Den Anwendungsbezug fand die Untersuchung bei neuartigen Betriebskonzepten der Bahntechnik, die auf dem Fahren im absoluten Bremswegabstand basieren. Anhand der durchgeführten Durchsatzanalysen und Fahrzeitermittlungen zur Fahrplankonstruktion und -optimierung wurden große Leistungspotentiale des neuen

Abstandhalteverfahrens bestätigt und die Nützlichkeit des entwickelten petrinetzbasierten Modellierungsansatzes gezeigt. Durch die Generierung von Evolutions- bzw. hybriden Erreichbarkeitsgraphen wurde eine geeignete Basis für die Analyse geschaffen, die zur Verifikation von Sicherheitseigenschaften der entwickelten Modelle herangezogen werden konnte. Im Rahmen der Arbeit von [Einer 2003] wurde gezeigt, wie Petrinetze zur Spezifikation und Analyse von Prozessen der Betriebsverfahren in der Eisenbahnsicherung verwendet werden können.

Petrinetze wurden auch im Rahmen der Entwicklung des europäischen Eisenbahnsicherungssystems ETCS (European Train Control System) als eine der ersten formalen funktionalen Beschreibungen eines Eisenbahnleitsystems eingesetzt, simuliert und verifiziert [Meyer zu Hörste et al. 1998, Meyer zu Hörste und Schnieder 1999]. Das formale Modell wurde insbesondere zur Validation der textuellen funktionalen Anforderungsspezifikation des Systems herangezogen, anhand dessen eine Reihe der Änderungen durch die Users Group des ETCS akzeptiert und eingearbeitet worden sind [Chalon et al. 1996, Schnieder 1998, Janhsen et al. 1997]. Diese Arbeiten mündeten in eine methodische Analyse und generische funktionale Modellierung von ELSS [Meyer zu Hörste 2003].

Die Formalisierung mit Petrinetzen beinhaltet auch die Modellierung der Verlässlichkeit des Bahnbetriebs, wie sie infolge von Störungen mit bekannter Häufigkeit entsteht, wobei mit Hilfe integrierter Petrinetzmodelle erste quantitative Analysen und Prognosen der Verlässlichkeit in Form von Leistungsbewertungen möglich wären [Zhu 2001, Zhu und Schnieder 2000a, Zhu und Schieder 2000b]. Für Dispositionsaufgaben im Bahnbetrieb wurde ein integriertes Fuzzy-Petrinetz Konzept entwickelt und für die wissensbasierte Disposition eingesetzt [Fay und Schnieder 1997, Fay und Schnieder 1998].

Die formale Systembeschreibung mit Petrinetzen bietet eine geeignete und einheitliche Basis für die Anwendung und Integration der unterschiedlichen Methoden der Sicherheitsanalyse [Cosulich et al. 1995]. Ein früher Ansatz, Petrinetze zur qualitativen Sicherheitsanalyse zu nutzen, findet sich bereits 1987 in [Leveson und Stolzy 1987], wobei diese Arbeiten allerdings nicht weitergeführt worden sind. Die Arbeiten von Trivedi beschränken sich weitgehend auf die Überführung von Fehlerbäumen in Petrinetzsysteme [Trivedi et al. 1993], allerdings nur unter strukturellen und weniger inhaltlichen Aspekten. Ein ähnlicher Ansatz wird in [Buchacker 2000] verfolgt: Neben der Definition einer formalen Semantik werden Fehlerbäume mit dem Ziel erweitert, Systemeigenschaften wie z.B. Ausfall- und Reparaturabhängigkeiten zwischen einzelnen Systemkomponenten zu erfassen. Die erweiterten Fehlerbäume werden auf stochastische Petrinetze (GSPN) [Marsan et al. 1995] abgebildet; der direkte Bezug zur Systemverlässlichkeit, zur Funktionalität und zum gesteuerten Prozess ist nicht integriert worden.

4.1.2 Grundlegender Formalismus

Petrinetze [Petri 1962] sind zur Beschreibung des dynamischen Verhaltens eines diskreten Ereignissystems in einer kausal-logischen Struktur geeignet. Die Systemstruktur ist als bipartiter Graph dargestellt, wobei die beiden disjunkten Knotenarten "Platz" und "Transition" in dem speziellen Netztyp der Bedingungs-Ereignis-Netze (BE-Netze) entsprechend als Bedingungen bzw. Ereignisse interpretiert werden [Starke 1990].

BE-Netze

Bedingungen für das Eintreffen eines Ereignisses sind stets erfüllt oder nicht erfüllt. Sie sind gleichzeitig Zustände des Systems, im Sinne von binären Aussagen, die zum betrachteten Zeitpunkt entweder wahr oder falsch sind. Ist eine Bedingung zu einem Zeitpunkt erfüllt (lokaler Zustand), so ist der dazugehörige Platz markiert. Die Menge aller zu einem Zeitpunkt erfüllten Bedingungen, respektive wahren Aussagen, repräsentiert den globalen Zustand des diskreten Ereignissystems.
Der kausale Zusammenhang zwischen Zuständen und Ereignissen wird durch gerichtete Kanten (Pfeile) dargestellt. Ein Ereignis ist aktiviert (eine Transition ist schaltfähig), wenn alle seine Vorbedingungen (Eingänge der Transition) markiert sind. Wenn ein Ereignis eintritt und so das diskrete Ereignissystem einer Zustandsänderung unterworfen wird, geht die aktuelle Markierung in eine neue über, indem die Marken der Vorbedingungen entfernt und die Nachbedingungen (Ausgänge der Transition) dagegen mit Marken belegt werden (s. Abbildung 4.1). Das Modell beschreibt somit nicht nur die Systemstruktur sondern auch das Systemverhalten! Soll eine der Bedingungen auch nach dem Schalten erfüllt bleiben, so ist sie mit entsprechender Transition über eine Doppelkante (Testkante) zu verbinden. Soll umgekehrt eine Transition dann schaltfähig sein, wenn eine Bedingung nicht erfüllt ist (der entsprechende Platz ist leer), dann ist dieser mit der Transition mit einem so genannten Inhibitor zu verbinden. Eine weitere Petrinetzklasse (S-T - Stellen-Transition Netze) erlaubt, dass ein Platz auch mit mehreren Marken markiert sein kann. Dadurch kann die Schaltfähigkeit einer Transition auch von der Anzahl der Marken abhängig gemacht werden, und eine Transition kann bei ihrem Schalten auch mehrere Marken generieren. Die entsprechende Anzahl der Marken wird als Kantengewicht der Kante zugeordnet.

Zeitbehaftete Petrinetze

In einem BE-Netz ist die Aktivierung eines Ereignisses als seine Bereitschaft zum Eintreten zu verstehen. In der allgemeinen Theorie der Petrinetze kann das Ereignis eintreten, muss es aber nicht. Um ergänzend die Zeitdauer zwischen Ereignissen modellieren zu können, kann in einem BE-Netz der Zeitbegriff eingeführt werden. Es wird hier ein

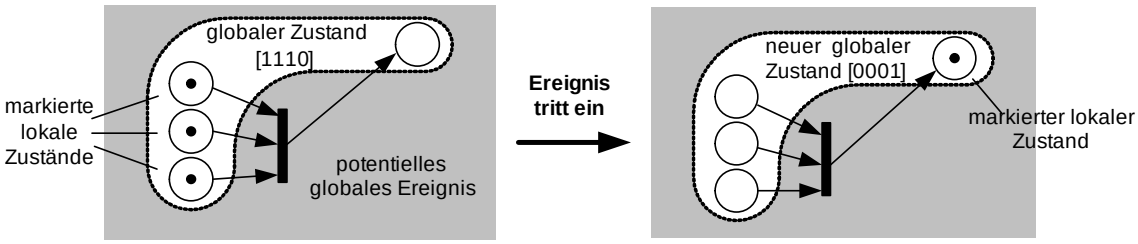

Abbildung 4.1: Dynamik im Petrinetz

Ansatz gewählt, der in mehreren Arbeiten zur Zeitbehaftung von Petrinetzen angewendet wird [Luttenberger und Cramer 1992, Schnieder 1999b, Zimmermann 1997]. Den Transitionen werden z.B. Zeitparameter zugewiesen. Der Zeitparameter θ einer Transition gibt an, wann die Transition nach ihrer Aktivierung schaltet. Während dieser Zeit bleiben die Vorbedingungen der Transition erfüllt, wenn sie nicht durch das Schalten einer anderen Transition verändert werden.
Vier charakteristische Typen des Zeitparameters θ sind zu unterscheiden:

- $\theta = 0$. Eine Transition dieses Typs schaltet nach dem Eintreten der Aktivierungsbedingung ohne Verzögerung (zeitlose oder kausale Transition). Diese Transition hat immer eine Priorität vor anderen Transitionstypen, die zu gleicher Zeit schaltfähig sind. Eine zeitlose Transition kann mit einem Wahrscheinlichkeitsgewicht W attributiert werden. Dieses wird berücksichtigt, falls zu einem Zeitpunkt mehrere zeitlose Transitionen aktiviert sein können. Eine kausale Transition t schaltet dann mit der Wahrscheinlichkeit $\frac{W_{t,M}}{\Sigma_{t'} W_{t',M}}$ wobei t' für alle schaltbaren kausalen Transitionen unter Markierung M steht.

- $\theta = T$. Eine Transition dieses Typs schaltet nach dem Eintreten der Aktivierungsbedingung genau nach Ablauf einer festen Verzögerungszeit T (deterministische Transition)

- $P(\theta \leq t) = 1 - e^{-\lambda t}$, wobei λ die Rate der Exponentialverteilung ist. Die Zeit, nach der eine Transition von diesem Typ schaltet, ist exponential verteilt und ihr Erwartungswert entspricht $1/\lambda$ (Transition mit exponentiellem Zeitverhalten).

- $P(\theta \leq t) = \Phi(t)$, wobei $\Phi(t)$ eine allgemeine stochastische Verteilungsfunktion ist. Die Zeit, die vom Eintreten der Aktivierungsbedingung bis zum Schalten der Transition vergeht, ist durch eine Wahrscheinlichkeitsverteilung beschrieben (allgemeine stochastische Transition).

Eine konkrete Klasse der zeitbehafteten Petrinetze bilden Erweiterte Deterministische und Stochastische Petrinetze (EDSPN - Extended Deterministic and Stochastic Petri

Nets) [German 1994]. Sie beinhalten alle vorher beschriebenen Komponenten inklusive der genannten temporalen Transitionsarten. Abbildung 4.2 zeigt die graphische Repräsentation aller Netzkomponenten der EDSPN's.

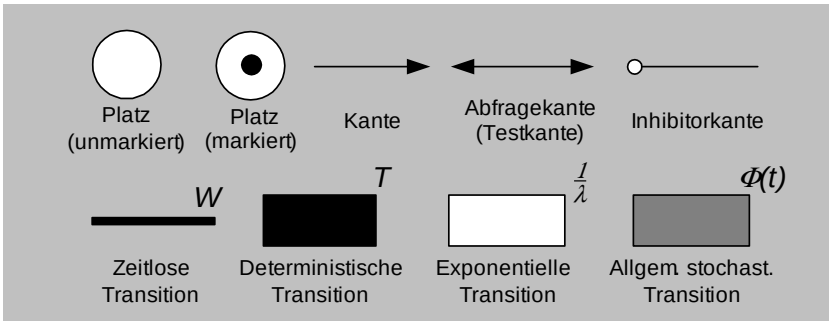

Abbildung 4.2: Graphische Netzkomponenten der EDSPN's

Hierarchie und Gefärbtheit

Eine nächste Erweiterung, verfügbar in der Netzklasse der Hierarchischen Gefärbten Petrinetze (HCPN - Hierarchical Colored Petri Nets) [Zimmermann et al. 1999] ermöglicht auf einer Seite eine Transition (so genannte Instanz oder Supertransitionen) mit einem Unternetz zu verfeinern. Die Eingangs- und Ausgangsplätze der Instanzen bilden dann die so genannten Ports des Unternetzes (vgl. Abb. 4.3).

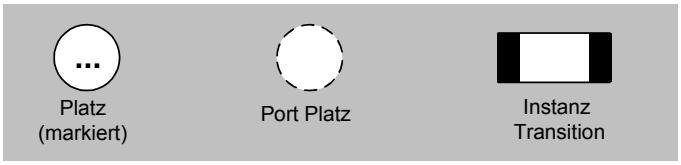

Abbildung 4.3: Hierarchische Netzkomponenten der HCPN's

Abbildung 4.4 zeigt das Beispiel einer Verfeinerung einer Instanz auf zwei hierarchischen Ebenen. Die Gewichtung der zeitlosen Transitionen *W1* und *W2* gibt die Wahrscheinlichkeit des Schaltens der allgemeinen stochastischen oder der deterministischen Transition auf der Unterebene an. Die Markierung der Portplätze der hierarchischen Unterebene entspricht der Markierung der Eingangs- bzw. Ausgangsplätze der Instanztransition (*P1* und *P2*).
Auf der anderen Seite bietet die Modellierung mit dieser Netzklasse eine Möglichkeit, mehrere Arten von Marken zu unterscheiden und dadurch die Schaltfähigkeit bestimmter Transitionen mit komplexeren Bedingungen ohne einen Zuwachs an Netzelementen

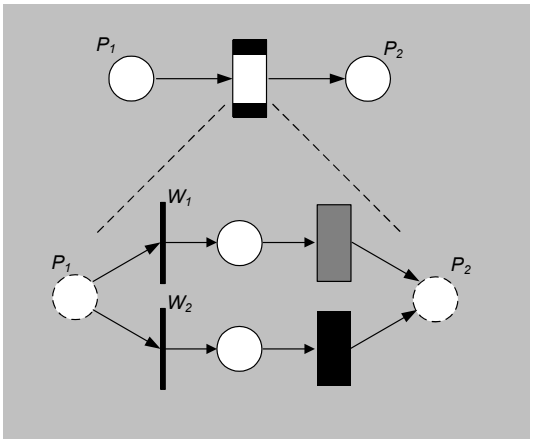

Abbildung 4.4: Beispiel der Verfeinerung einer Instanztransition

zu realisieren. Die Gefärbtheit ermöglicht es auch einer Transition mehrere Zeitparameter (oder stochastische Verteilungen) zuzuordnen und diese je nach der Farbe der Markierung auf den Eingangsplätzen dann für das Schalten anzuwenden.

4.1.3 Analysemethoden

Dank des ausgereiften mathematischen Hintergrunds bieten Petrinetze eine Reihe von formalen Analysemöglichkeiten. Aus Sicht der Anwendung für Sicherheitsanalysen können diese als qualitativ oder quantitativ klassifiziert werden (s. Kapitel 3.2.2).

Qualitative Analysemöglichkeiten Hier zugehören insbesondere alle Analysearten die auf der Generierung des Erreichbarkeitsgraphen basieren. Ein Erreichbarkeitsgraph besteht aus Knoten und Kanten, wobei jeder Knoten einen Globalzustand beschreibt, der einer bestimmten Markierung des Petrinetzes entspricht. Eine Markierungsänderung ist in der Darstellung des Erreichbarkeitsgraphen durch den Übergang mittels einer Kante von einem Knoten zu einem anderen gegeben. Weil eine Markierungsänderung im Petrinetz durch das Schalten einer Transition erfolgt, ist jede Kante des Erreichbarkeitsgraphen einer Transition zugeordnet. Der Erreichbarkeitsgraph repräsentiert dadurch den gesamten Zustandsraum des Verhaltens des Systems, das durch das Petrinetz beschrieben wird. Da der Erreichbarkeitsgraph ausschließlich globale Zustände beinhaltet, entspricht seine Struktur dem Zustandsautomaten des beschriebenen Systems. Eine Generierung des Erreichbarkeitsgraphen aus einem Petrinetz erfolgt meist automatisch. Da der Erreichbarkeitsgraph in den meisten Fällen sehr groß wird und daher seine visuelle Analyse praktisch nicht möglich ist, werden hierzu Algorithmen verwendet. Zu den Algorithmen gehören:

- Analyse der Erreichbarkeit eines bestimmten Zustandes. Hierbei wird überprüft, ob ein bestimmter Systemzustand von einem Anfangszustand ausgehend im modellierten Systemverhalten erreichbar ist.

- Rückwärts- oder Vorwärtsanalyse des Erreichbarkeitsgraphen. Hierbei werden die Vor- oder Folgezustände bzw. Zustandsübergänge eines bestimmten Systemzustands ermittelt.

- Analyse globaler relevanter Zustandsmengen. Es werden alle Zustände mit einer charakteristischen Eigenschaft des Zustandsraumes ermittelt. Diese Eigenschaft ist durch Markierung eines bestimmtes Platzes (oder Plätze) definiert.

- Analyse der Zustandsbedingungen einer Zustandsmenge. Alle Markierungen einer globalen Zustandsmenge werden mit dem Ziel untersucht, die Auftrittsbedingungen in Form von möglichen Markierungen der Elementarplätze zu ermitteln.

Weitere qualitative Analysemöglichkeiten, die nicht auf der Berechnung des Erreichbarkeitsgraphen basieren, bietet die Berechnung von P- und T- Invarianten. Im Falle der Analyse der P-Invarianten kommen als Ergebnis Gewichte für Plätze des Petrinetzes heraus. Die auf dieser Weise gewichtete Tokensumme bleibt für alle erreichbaren Zustände konstant. Die P-Invariantenanalyse führt daher zur Identifikation von Gleichgewichts- und Beschränkheitsaussagen. Ist ein Platz in einer P-Invariante enthalten, können Aussagen über seiner maximal höchster Markiertheit getroffen werden. Die Berechnung von T-Invarianten ermittelt für Transitionen mögliche Schalthäufigkeiten. Diese reproduzieren Markierungen vorausgesetzt, dass die T-Invarianten realisiert werden können (d.h. es muß eine Schaltsequenz geben, die unter der bestimmten Markierung äktiviertïst). Auf dieser Weise können also innerhalb der Prozess-, Funktionalitäts- oder Verlässlichkeitsmodellierung Ablaufszenarien identifiziert und mit dem gewünschtem Verhalten verglichen werden.

Quantitative Analysemöglichkeiten Hierzu gehören alle Analysetechniken, die die Auftrittswahrscheinlichkeit bestimmter Markierungen eines Platzes oder die Aktivierungshäufigkeit (Rate) einer bestimmten Transition ermitteln. In Abhängigkeit des Bezugszeitpunkts der quantitativen Ergebnisse wird unterschieden zwischen der

- stationären Analyse, die die Ergebnisse in Bezug auf das eingeschwungene Systemverhalten ($t \rightarrow \infty$) ermittelt und der

- transienten Analyse, bei der die Ergebnisse zu einem beliebigen Zeitpunkt ($t = T$) oder auf ein Zeitintervall ($t \in [T_1; T_2]$) bezogen sind.

Die Ergebnisse der stationären oder transienten Analyse können numerisch entweder analytisch oder simulativ errechnet werden. Obwohl das analytische Verfahren meistens zu sehr genauen Ergebnissen führt, ist es mit großen strukturellen Begrenzungen der Modellierung (z.B. keine parallele Aktivierung von zwei deterministischen Transitionen, Verwendung ausschließlich von exponentiellen stochastischen Verteilungen) verbunden. Die allgemein immer einsetzbare Simulation dagegen kann, insbesondere bei der Berechnung von Häufigkeiten von selten auftretenden Zuständen oder schaltenden Transitionen, zu ungenügender Genauigkeit oder zu langen Auswertungszeiten führen. Eine Lösung bieten Verfahren der Simulation von seltenen Ereignissen wie z.B. RESTART/Importance splitting, Importance Sampling, Cross-Entropie usw. [Garvels und Rubinstein 2001, Haraszti und Townsend 1999] oder ein in [Slovák et al. 2005] beschriebenes Verfahren, das auf der Approximation und Extrapolation der Verläufe der quantitativen Ergebnisse basiert.

4.1.4 Toolunterstützung

Die Toolunterstützung zur praktischen Anwendung der genannten Klasse der Petrinetze im behandelten *PROFUND*-Vorgehen besitzt derzeit noch mehrere Schwachstellen.
Von den heuzutage zugänglichen Tools bietet zur Modellbildung und zur quantitativen Analyse mit Ausnutzung analytischer bzw. simulativer Lösungen TimeNET 3.0.5 [TimeNET] die beste Funktionalität. TimeNET 3.0.5 unterstützt die Modellierung mit der Klasse der EDSPN's sowie die Möglichkeit der Bildung von hierarchischen Modellen und Verwendung von farbigen Marken für die Klasse der stochastischen HCPN. Das wesentlich breitere und leistungsfähigere Spektrum der Analysemöglichkeiten der EDSPN hat zur Folge, dass die hierarchischen HCPN-Modelle oft zu transformieren (leider manuell) und als flache EDSPN Netze zu analysieren sind.
Die durch die quantitative Analyse ermittelten Daten können in MS Excel weiter verarbeitet werden. Dies betrifft insbesondere die Darstellung graphischer Verläufe und Approximation sowie Extrapolation der erhaltenen Abhängigkeiten durch mathematische Gleichungen.
Da TimeNET eine Generierung des Erreichbarkeitsgraphen nicht unterstützt, sind zur qualitativen Analyse weitere Tools heranzuziehen. Die Tabelle 4.1 zeigt die Eigenschaften der Tools, die zur Entwicklung und praktischen Anwendung der *PROFUND*-Methode benutzt worden sind (markiert ist jeweils die verwendete Funktionalität des Tools).
Das Tool iVA-PN-Analyser stellt eine erste Implementierung der Allgorithmen dar, die ausschließlich zu dem Zweck der Sicherheitsanalyse nach der *PROFUND*-Methode am Institut für Verkehrssicherheit und Automatisierungstechnik der TU Braunschweig entwickelt wurden (s. Kapitel 6) Neben einer Visualisierung und Untersuchung des

	Herkunft	PN Klassen	Gefärbt-heit	Hierar-chie	Modula-rität	Simula-tion	Numeri-sche Analyse	Invarian-ten	Erreich-barkeits-graph	Graph Mengen globaler Zustände	Unfall-baum
TimeNET 3.0.5	TU Berlin (D)	EDSPN HCPN	+	+	-	+	+	o	-	-	-
Design CPN	University of Aarhus (DK)	CPN	+	+	+	+	-	-	+	-	-
SPNP	Durham University (USA)	SPN	o	-	+	o	o	-	+	-	-
iVA-PN-Analyser	TU Braun-schweig (D)	-	-	-	-	-	-	-	-	+	+
Poseidon	Universität Koblenz-Landau (D)	S/T	-	+	-	+	-	+	-	-	-

Tabelle 4.1: Bewertung der bei der PROFUND Methode angewendeten Tools (+ - gut geeignet, o - beschränkt geeignet, – - ungeeignet)

Erreichbarkeitsgraphen (generiert aus dem SPNP-Tool [SPNP]) ist es möglich, den iVA-PN-Analyser zur Generierung der Graphen der Mengen globaler Zustände und der Unfallbäume anzuwenden.

4.2 Bezug der Petrinetze zu Beschreibungsmitteln der Sicherheitsanalyse

Obwohl die Petrinetze auf den ersten Blick einen sehr unterschiedlichen Formalismus gegenüber den beschriebenen traditionellen Beschreibungsmitteln der Sicherheitsanalyse zu haben scheinen, bestehen einige eindeutige Beziehungen, die eine Basis zur Transformation darstellen.

PN → Markovkette Hier besteht ein eindeutiger Bezug, der zwischen dem Erreichbarkeitsgraphen und der entsprechenden Markovkette dann existiert, wenn das stochastische Petrinetz ausschließlich temporale Transitionen mit Exponentialverteilungen beinhaltet. Die zusätzliche Verwendung der kausalen (zeitlosen) Transitionen (Klasse der GSPN) ist ebenso zulässig, um eine automatische Transformation des Perinetzes in eine Markovkette durchführen zu können [Marsan et al. 1995]. Die quantitative Analyse des Petrinetzes ermittelt die gleichen Ergebnisse wie die Analyse der Markovkette. Ein Vergleich der beiden Formalismen aus [Stoytcheva et al. 2005] zeigt die Abbildung 4.5.
Die Darstellung der Markovkette als Petrinetz ist meistens wesentlich überschaubarer, weil das Petrinetz die Beschreibung von Lokalzuständen ausnutzt. Im Gegensatz zu

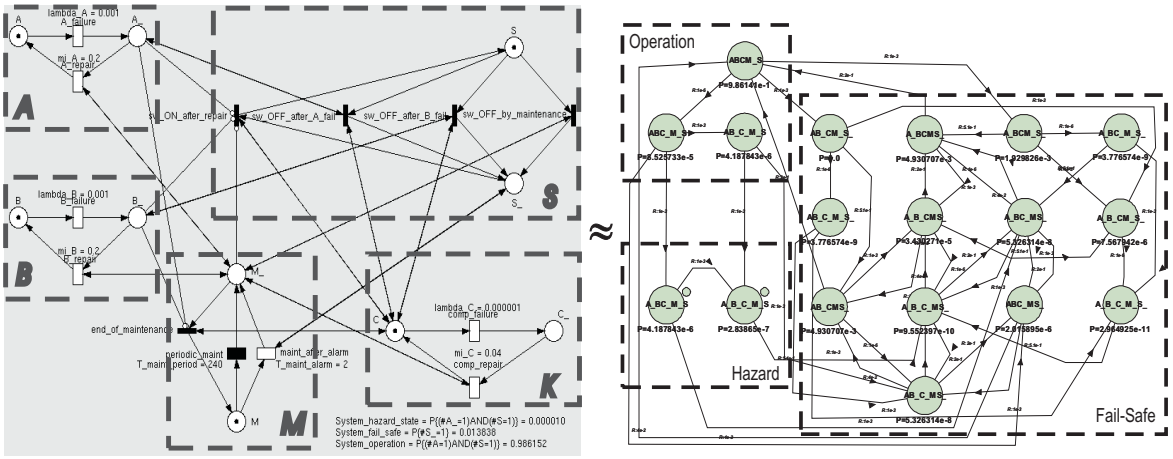

Abbildung 4.5: Petrinetz und die entsprechende Markovkette

Markovketten ist mit Petrinetzen auch die Beschreibung von deterministischen und allgemeinen Ereignissen des Systemverhaltens möglich, die dann allerdings nicht mehr in Markovketten überführt werden können. Eine Approximation der allgemeinen stochastischen Verteilungen durch Phasenverteilungen ermöglicht die vorteilhafte numerisch analytische Lösung für die Auswertung auszunutzen [Kassev et al. 2006].

PN → ETA Dieser Bezug existiert nur dann, wenn das Petrinetz als Graph der Mengen globaler Zustände dargestellt ist, wobei die charakteristischen Eigenschaften der Zustandsmengen durch sicherheitsrelevante Plätze des Petrinetzes (der ETA entsprechend) definiert sind (z.B. Plätze, die die Gefährdungen, gefährliche Situationen und Unfälle repräsentieren). Die automatisch generierten Übergänge zwischen den globalen Zustandsmengen entsprechen den Ereignissen die Gegenstand des Interesses der Ereignisbaumanalyse (ETA) sind (s. Beispiel in Abbildung 5.3 in Kapitel 5 - Analyse). Die quantitative Analyse des Petrinetzes ermöglicht, die ereignisbaumspezifischen quantitativen Ergebnisse zu ermitteln.

PN → FTA Dieser Bezug entsteht durch eine Analyse der Zustände einer globalen Zustandsmenge (gebildet aus dem Erreichbarkeitsgraph eines Petrinetzes), deren charakteristische Eigenschaft durch einen sicherheitsrelevanten Platz definiert ist (Gefährliche Situation oder Unfall), der dem Top-Zustand des Fehlerbaumes entspricht. Durch die Analyse der Markierungen aller Zustände der globalen Zustandsmenge unter Berücksichtigung des hierarchischen Aufbaus des Petrinetzmodells können die logischen Beziehungen unter einzelnen Ursachen des Top-Zustandes (inklusive minimaler Cut-Sets) herausgefunden werden (s. Beispiel auf der Abbildung 6.10). Die quantitative

Analyse des Petrinetzes ermöglicht die fehlerbaumspezifischen quantitativen Ergebnisse zu ermitteln. Im Gegensatz zur traditionellen Fehlerbaumanalyse wird hier bei der Auswertung das dynamische Verhalten des modellierten Systems integriert.

PN → RBD Obwohl hier kein direkter Bezug zu bezeichnen ist, kann grundsätzlich gesagt werden, dass durch systemkomponentenspezifische Petrinetzmodellierung die gleichen Fragestellungen (Untersuchung der Zuverlässigkeitsstrategien) wie bei den Zuverlässigkeitsblockdiagrammen (engl.: Reliability Block Diagram - RBD) beantwortet werden können. Durch Modellierung der Verhaltensdynamik mit Hilfe von Petrinetzen können diese Fragen auch in Richtung von Wartungs- und Diagnostikstrategien erweitert werden.

4.3 Vergleich der Petrinetze mit Beschreibungsmitteln der Sicherheitsanalyse

Tabelle 4.2 zeigt den Vergleich der Eigenschaften der traditionellen Beschreibungsmittel und der Petrinetze (hier basierend auf der Klasse HCPN).

4.4 Zusammenfassung

Die Vergleichstabelle 4.2 zeigt deutlich, dass die Petrinetze das Potential aller erforderlichen Eigenschaften eines Beschreibungsmittels für die Sicherheitsanalyse besitzen. Das notwendige Fachwissen und die nicht vorhandene spezifische Toolunterstützung sind ständige Ursachen nur mäßiger Akzeptanz unter Anwendern aus der Praxis. Eine bedeutende Barriere der Ausbreitung der Petrinetze im Bereich der Sicherheitsanalyse basiert auf einer bislang ausgebliebenen Methode, die dem Anwender durch klare Vorgehensvorschriften und Beispiele das Fachwissen nahe bringen würde. Die vorliegende Arbeit hat das Ziel, einen Beitrag in diese Richtung zu leisten.

Beschreibungsmittel / Methode	Für komplexe Systeme geeignet	Für neue Systementwürfe geeignet	Qualitative Analyse (Zustandsraum)	Quantitative Analyse (Wahrscheinlichkeiten, Raten)	Quantitative Analyse (Stochastische Verteilungen)	Simulation	Für Kombinationen von Ausfällen geeignet	Zur Betrachtung von Reihenfolgeabhängigkeiten geeignet	Bottom-Up- oder Top-Down-Methode	Für Zuordnung von Sicherheitsanforderungen geeignet	Fachwissen erforderlich	Akzeptanz und Gebräuchlichkeit	Tools erforderlich	Plausibilitätsprüfungen	Verfügbarkeit von Tools	IEC-Norm
ETA	-	-	-	o	-	o	-	+	B-U	-	o	o	o	+	o	-
FMECA	-	-	-	o	-	-	-	-	B-U	-	+	+	o	+	+	60812
FTA	+	+	-	+	-	-	+	-	T-D	+	o	+	o	+	+	61025
HAZOP	-	-	-	-	-	-	-	-	B-U	-	o	o	o	+	o	61882
Markov	o	o	o	-	+	o	+	+	T-D	+	-	o	-	-	o	61165
RBD	+	-	o	+	+	-	+	-	T-D	+	-	o	o	+	o	61078
PN/ProFunD	+	+	+	+	+	+	+	+	T-D	+	-	-	-	+	o	15909

Tabelle 4.2: Bewertung der in der Sicherheitsanalyse meistens angewendeten Methoden in Anlehnung nach [Braband2005] und deren Vergleich mit Petrinetzen (+ - gut geeignet, o - beschränkt geeignet, – - ungeeignet, B-U - Bottom-Up, T-D - Top-Down)

Kapitel 5

PROFUND-Modellierung

5.1 Grundlegendes Konzept

Um eine ausreichende Genauigkeit der stochastischen Auswertung zu erreichen, ist ein holistischer Ansatz der Beschreibung aller beitragenden Risikofaktoren notwendig. Das grundlegende Konzept der hier vorgestellten *PROFUND*-Methode zur Sicherheitsanalyse von Eisenbahnsystemen sieht vor, für alle Einflussfaktoren des Risikos im Eisenbahnbetrieb ein einziges formales Beschreibungsmittel zu verwenden. Dies betrifft sowohl den gesteuerten Verkehrsprozess, in welchem das Potential für Auftritte von unerwünschten Ereignissen besteht, als auch die Funktionalität und Verlässlichkeit des ELSS, dessen Aufgabe es ist, den Verkehrsprozess zu steuern und das untolerierbare betriebliche Risiko zu vermeiden.
Zur Beschreibung der relevanten Prozesse im Betrieb und Steuerungssystem der Eisenbahn werden in dieser Arbeit die EDSPN als formale Modellierungssprache verwendet (s. Kapitel 4). In den folgenden Unterkapiteln werden die Ansätze zur Anwendung dieser Modellierungssprache in allen Ebenen der Beschreibung (Prozess, Funktionalität, Verlässlichkeit) vorgestellt. Als Unterstützung der Erläuterung des methodischen Vorgehens wird anhand praktischer Beispiele aus Strecken- und Bahnhofssicherung die Anwendbarkeit des methodischen Vorgehens gezeigt.
Abbildung 5.1 zeigt die einzelnen Schritte der Anwendung der *PROFUND*-Methode mit dem Verweis auf das entsprechende Unterkapitel dieses Kapitels, in dem eine detaillierte Erläuterung zu finden ist.

5.2 Systemgefahrenanalyse

Basis für jede Systembeschreibung zum Zweck der Risikobewertung ist eine Gefahrenanalyse, im deren Rahmen die relevanten Gefahren des Eisenbahnbetriebes entspre-

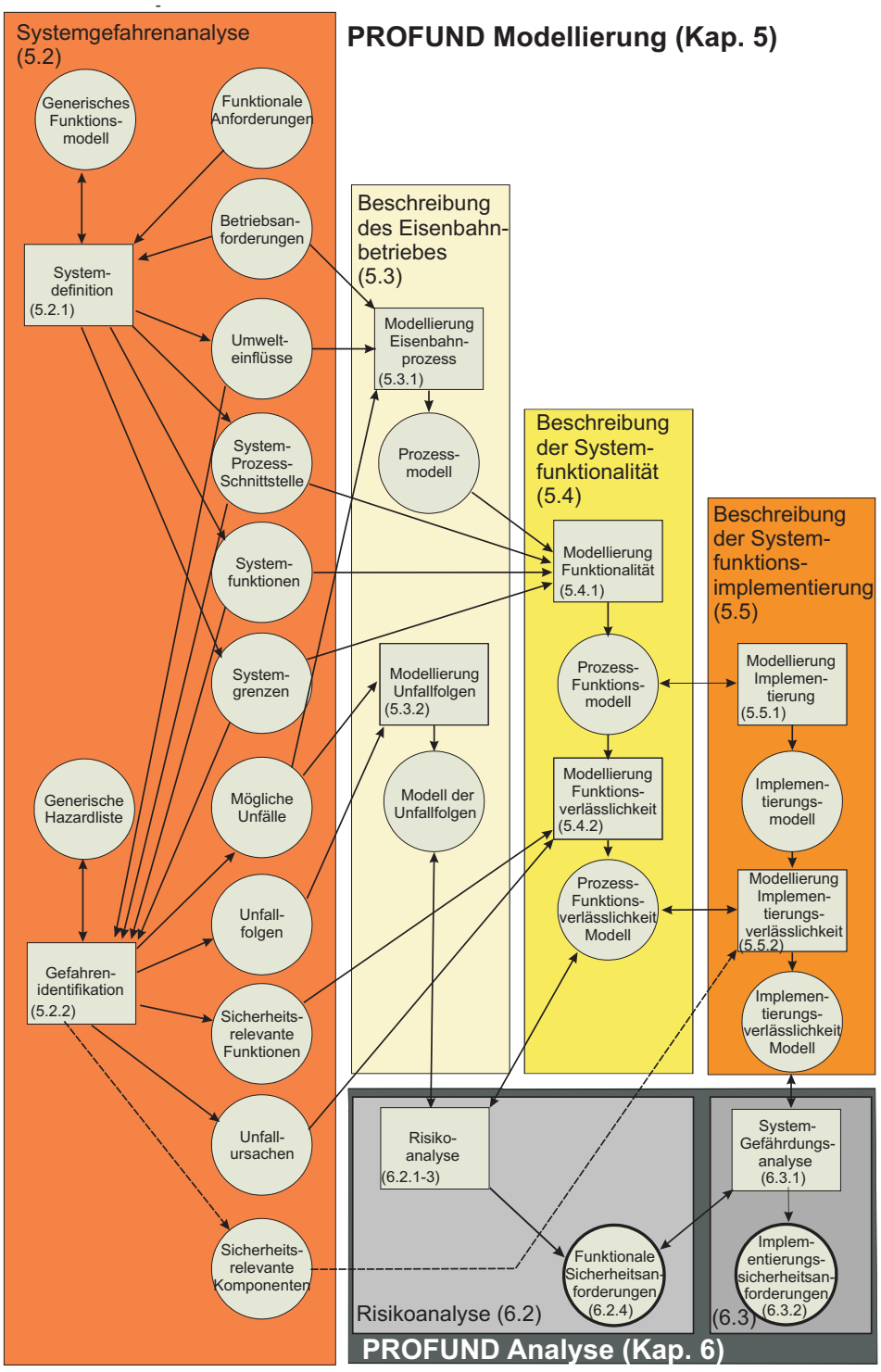

Abbildung 5.1: Vorgehen bei der Anwendung der *PROFUND*-Methode für die Definition der Sicherheitsanforderungen auf die Systemfunktionalität und -implementierung

chend den Systemgrenzen identifiziert werden.
Um eine Gefahrenanalyse durchführen zu können, ist es im ersten Schritt notwendig, die Grenzen des zu analysierenden Systems zu definieren und das sich aus seinem Betrieb ergebende Gefahrpotential qualitativ zu identifizieren. Dies kann im Rahmen einer Systemdefinition und einer anschließenden Gefahrenidentifikation erfolgen.
Eine Gefahrenanalyse für den Betriebseinsatz eines sicherheitsrelevanten Systems kann entweder auf der typbezogenen oder der exemplarbezogenen Ebene durchgeführt werden. Während bei der meistens durch Hersteller vorab durchgeführten typbezogenen Gefahrenanalyse von maximalen Parametern des zu steuernden Betriebes ausgegangen wird, bezieht sich die exemplarbezogene Analyse auf die konkreten topologischen und leistungsbezogenen Parameter des Betriebes, für den der Einsatz des Systems vorgesehen ist. Dabei soll nicht außer Acht gelassen werden, dass die Zulassung eines Eisenbahnsystems auf einem exemplarbezogenem Nachweis der Sicherheit basiert.

5.2.1 Systemdefinition

Im Sinne der *PROFUND*-Methode beinhaltet die Aufgabe der Systemdefinition die Identifikation der Grenzen und Schnittstellen des betrachteten Systems sowohl auf der Ebene des Eisenbahnprozesses als auch auf der Ebene der Systemfunktionen bzw. der Systemimplementierung.
Auf der Ebene des Eisenbahnprozesses ist es insbesondere die geographische Auslegung des zu analysierenden Teils des Verkehrssystems mit Beschreibung aller spezifischen Betriebsbedingungen und möglichen Umwelteinflüssen. Unter diesen Aspekten sollte z.B. die Infrastruktur, das Verkehrsaufkommen, Spektrum der Geschwindigkeiten der Verkehrsfahrzeuge oder die Interaktion mit der Umwelt analysiert werden.
Auf der Ebene der Systemfunktionalität ist es die Identifikation der betrieblichen Funktionen, die für die Steuerung und Sicherung des Eisenbahnprozesses vorgesehen sind. Hierunter fällt die Dokumentierung der funktionalen Systemgrenzen mit der Identifikation der Nachbarsysteme und der gegenseitigen Schnittstellen. Neben der Auflistung der durch das System zu realisierenden Funktionen sind auch die Funktionen, die durch menschliches Bedienpersonal übernommen werden, zu beschreiben. Dieses soll sowohl im Regelbetrieb als auch im degradierten Betrieb betrachtet werden.
Ein wichtiger Teil der Systemdefinition ist die genaue Beschreibung der Interaktion zwischen dem Eisenbahnprozess und der Systemfunktionalität. Hier ist auch eine besondere Aufmerksamkeit der menschlichen Rolle zu widmen.
Als Grundlage für die Identifikation der Systemfunktionalität kann das durch die AEIF (Association Européen d'Interopérabilité Ferroviaire) [AEIF 2002] erstellte funktionale Modell des Eisenbahnsystems herangezogen werden. Ebenfalls können andere Systemmodelle zu Grunde gelegt werden, z.B. das generische Modell von Eisenbahnleit- und

-sicherungssystemen von [Meyer zu Hörste 2003]. Abbildung 5.2 zeigt eine solche mögliche Strukturierung der Funktionalität, die in dieser Arbeit zu Grunde gelegt wurde.

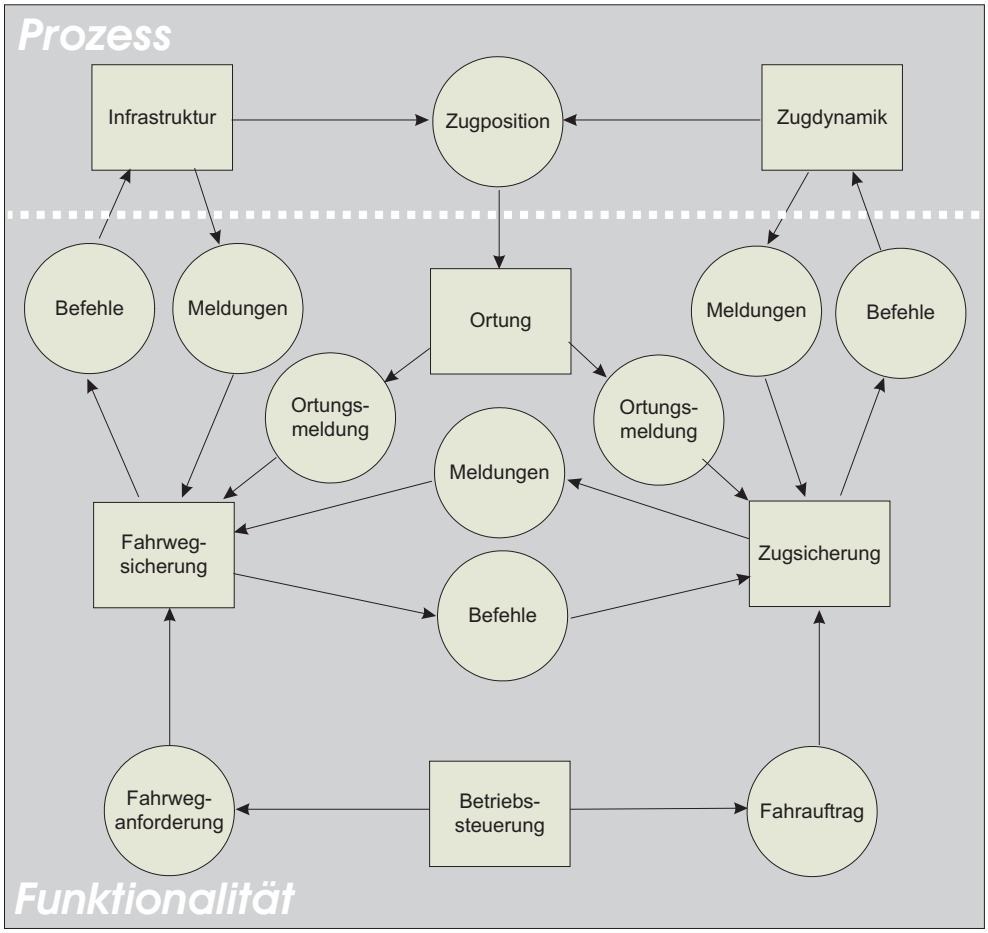

Abbildung 5.2: Eisenbahnsystemmodell in Anlehnung an [Meyer zu Hörste 2003]

5.2.2 Gefahrenidentifikation

Als eine Gefahr (engl. Hazard) wird durch die Norm EN 50 126 *die physikalische Situation* bezeichnet, *die ein Potential für eine menschliche Verletzung besitzt.* In dem ersten Entwurf der praktischen Anweisung zur Anwendung der EN 50126 [prTR50126-2 2005] wird empfohlen, den Begriff "physikalische Situation" durch den allgemeineren Begriff "*Bedingung*" zu ersetzen.
Im Sinne der *PROFUND*-Methode sind die Ergebnisse der Gefahrenidentifikation einerseits die gefährlichen Betriebssituationen, die zu den grundsätzlich unerwünschten

Ereignissen des Eisenbahnbetriebes (z.B. Entgleisung und Kollision, s. Kapitel 2) führen können. Von Bedeutung ist dabei auch die probabilistische Abschätzung, dass die Situation tatsächlich zum Unfallereignis führt. Aus Sicht der Sicherheit ist es oft notwendig, bei der Quantifizierung des Ereigniseintritts die *Worst Case* Betrachtung zu berücksichtigen.
Auf der anderen Seite ist im Rahmen der Gefahrenidentifikation die Funktionalität des ELSS mit dem Ziel zu untersuchen, die Systemfunktionen zu finden, deren Versagen zu der jeweiligen gefährlichen Betriebssituation geführt hat. Als Grundlage kann die vorläufige funktionale Spezifikation des ELSS (falls bereits vorhanden) verwendet werden. Im anderen Fall (z.B. bei der Entwicklung neuartiger Systeme) ist auf eine generische Funktionsmodellierung des Eisenbahnsystems zurückzugreifen [AEIF 2002] [Meyer zu Hörste 2003].
Eine Art Gefahrenidentifikation muss auch in der Phase der Systemherstellung im Rahmen der technischen Spezifikation durchgeführt werden. Hier besteht die Aufgabe, alle Komponenten der Systemimplementierung zu identifizieren, die zum einem Gefahrzustand der implementierenden Funktion führen können.
Für die Durchführung der Gefahrenidentifikation kann eine Reihe von Methoden angewendet werden. Die Anweisung prTR 50126-2 empfiehlt empirische Gefahrenidentifikation unter Verwendung z.B. von Checklisten oder FMEA [Gralla und Heinz 1998] oder kreative Gefahrenidentifikation mit Einsatz von Brainstorming oder HAZOP [Fenelon et al. 1995]. Eine völlig konsequente Durchführung der Gefahrenanalyse, auch im Sinne der allgemein angestrebten europäischen Interoperabilität, kann nur unter Verwendung einer generischen Hazardliste erreicht werden, wie sie z.B. für das Projekt Eurointerlocking erarbeitet wurde [Pope et al. 2006].
Für die Identifikation der kausalen Zusammenhänge der unerwünschten Betriebsereignisse (Unfälle) mit deren Ursachen im Betriebsprozess und in der Systemfunktionalität sind die Ansätze der Top-Down Analyse wie z.B. Störungsbaumanalyse (*FTA - Fault Tree Analysis* [Vesely et al. 1981]) vorbestimmt.
Abbildung 5.3 zeigt den Störungsbaum der Gefahrenanalyse einer als Beispiel genommenen Strecke in der Länge von mehreren Streckenabschnitten. Als Top-Event wurde die *Kollision* zweier Züge (Auffahren) untersucht, wobei als unmittelbar davor stehende gefährliche Situation die Präsenz von zwei Zügen in einem Streckenabschnitt identifiziert wurde. Der Störungsbaum wird im Rahmen der Risikoanalyse des Systems weiter auf die Funktionsebene entwickelt. In der Phase der Definition der technischen Systemanforderungen kann die Entwicklung auf der Implementierungsebene fortgesetzt werden.
Neben der Analyse der weiteren Kollisionsarten könnte auch der Störungsbaum des zweiten grundlegenden unerwünschten Betriebsereignisses *Entgleisung* auf ähnliche Weise aufgebaut werden, wobei die konkreten geografischen Parameter der Strecke in Be-

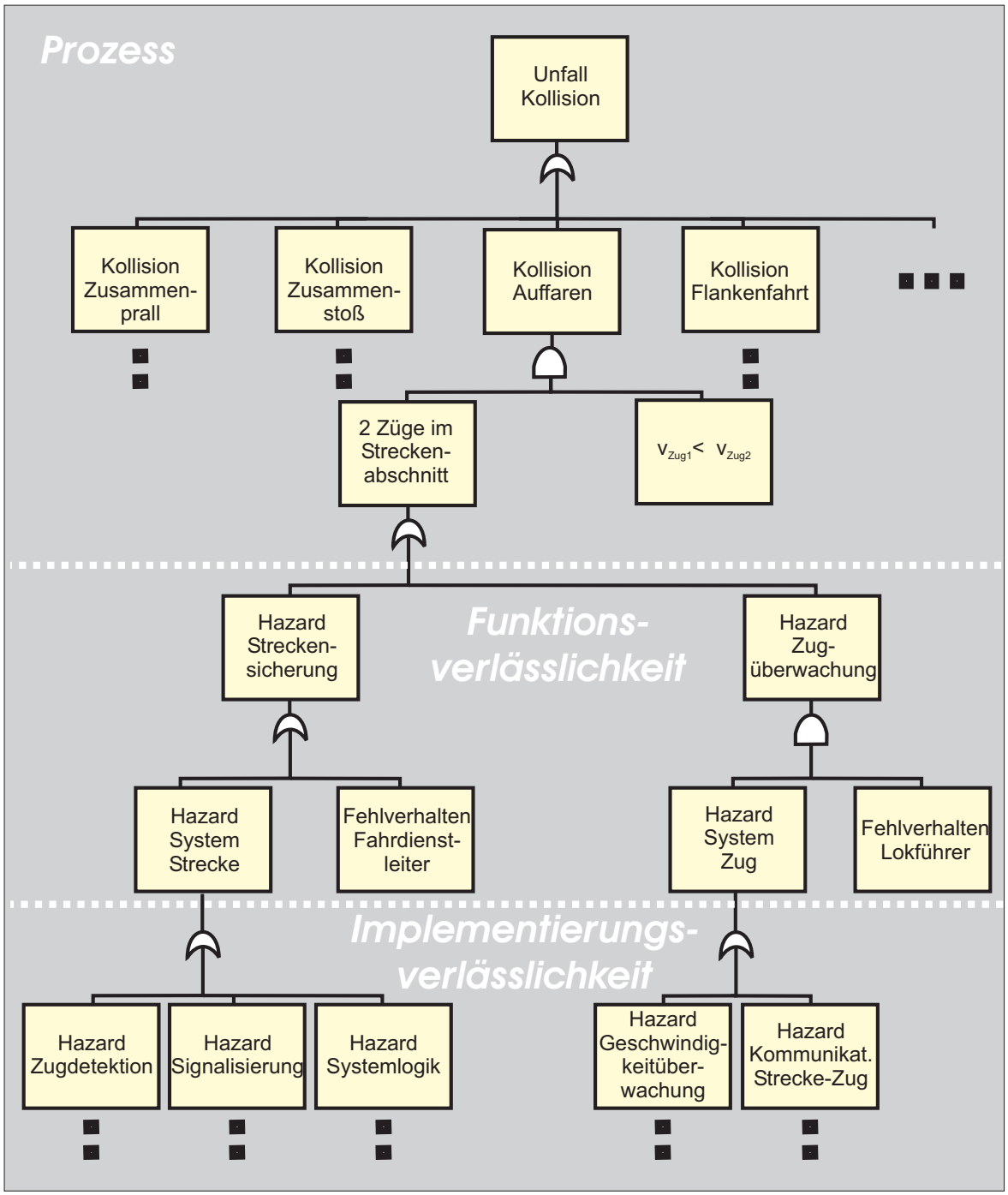

Abbildung 5.3: Störungsbaum für eine Kollision auf einer eingleisigen Strecke

tracht zu ziehen sind. In dem angenommenen Beispiel gehören hier z.B. die streckenabschnittbezogenen Geschwindigkeitsbegrenzungen, bei deren Überschreitung das Potenzial für Zugentgleisungen besteht.

5.3 Beschreibung des Eisenbahnbetriebes

Die risikobasierte Definition der Sicherheit setzt voraus, dass als Grundlage für die Sicherheitsanalyse jedes Systems im Eisenbahnbereich eine ausführliche Analyse des Betriebsprozesses durchgeführt wird. Die Durchführung dieser Aufgabe erfordert eine ausreichende Kenntnis der Eisenbahndomäne, um alle relevanten Betriebsabläufe in Betracht zu ziehen und die unerwünschten Betriebsereignisse (Unfälle) und Gefahren vollständig zu identifizieren. Dabei sollte sich die Analyse auf die Betriebsprozesse richten, für deren Steuerung das untersuchte System bestimmt ist. Die Gefahrenanalyse des Betriebsprozesses (Unterkap. 5.2) ist daher eine Grundlage für die Modellierung, hilft jedoch oft auch zu deren Identifikation.

5.3.1 Modellbildung - Verkehrsprozess

Ziel der Modellierung des Betriebsprozesses ist es, den Bezug zwischen den gefährlichen Situationen und den unerwünschten Betriebsereignissen kausal und temporal zu beschreiben. Basis der Modellierung bilden die betrieblichen Prozesse, die die identifizierten gefährlichen Situationen beinhalten und somit zu den unerwünschten Ereignissen führen können. Eine reine prozessbezogene Betrachtung ermöglicht das tatsächliche, sich aus dem Prozess ergebende Risikopotential zu identifizieren. In ersten Schritt der Modellierung ist daher davon auszugehen, dass das Betriebsverhalten durch keine systembezogenen Eingriffe d.h. weder reguläre, noch systemstörungsbasierte, beeinflusst wird.
Die Beschreibung des Betriebsprozesses baut auf der ablauforientierten Modellierung auf, wobei die einzelnen Betriebsszenarien in betriebliche Situationen und betriebliche Ereignisse zerlegt werden. Eine bestimmte betriebliche Situation wird im Modell dann eingenommen, wenn der zugehörige Platz mit einem bzw. mehreren Token belegt ist. Durch die Nutzung der höheren stochastischen Petrinetze ist es möglich, die betriebliche Situation nicht nur durch die Anzahl der vorhandenen Token, sondern auch durch die Tokenart (Farbe) zu konkretisieren. Abbildung 5.4 zeigt ein abstraktes Beispiel der Betriebsmodellierung, in dem nach Auftritt eines bestimmten Betriebsereignisses (*Operation-event2*) eine gefährliche Situation entsteht. Durch eine probabilistische Gewichtung der kausalen Transitionen (*Near-miss-event* und *Accident-event*) können verschiedene potentiellen Folgen differenziert werden.

Durch Verwendung von Abfragekanten und Inhibitoren können in den modellierten Betriebsprozes bedingte Ereignisse (*Operation-event6*) oder Entscheidungen (*Operation-event5*) integriert werden.

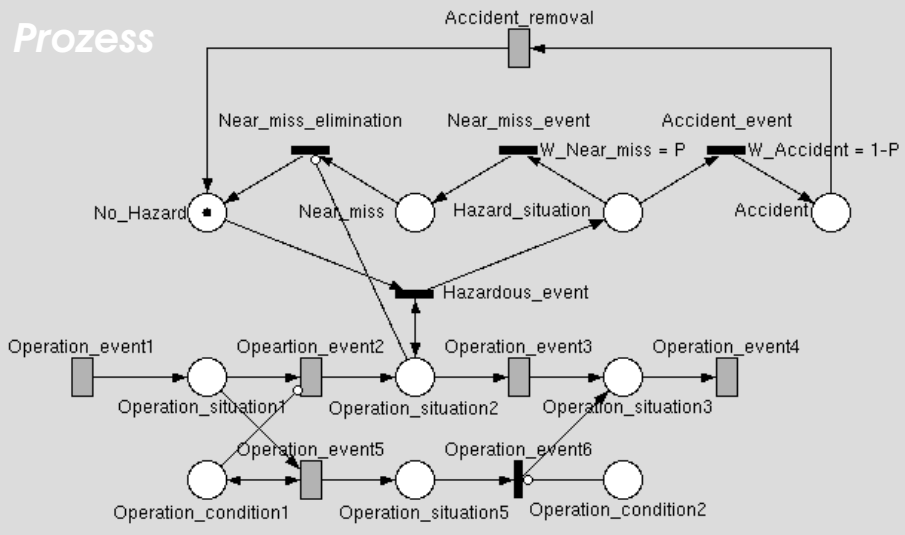

Abbildung 5.4: Beispiel der Modellierung eines Betriebsablaufs mit potentiellen Unfallfolgen.

Die Komplexität der Modellierung ist einerseits durch den Bezug zu dem untersuchten System, andererseits durch den Grad der Verfügbarkeit und Genauigkeit der statistischen Daten und der Daten aus der Gefahrenanalyse gegeben. In der hier vorliegenden Arbeit wurde das System der Eisenbahn als ein diskretes Ereignissystem betrachtet. Es wird davon ausgegangen, dass, obwohl in dem System kontinuierliche Prozesse ablaufen, es ist immer möglich ist, eine ausreichende Diskretisierung des Verhaltens als ein quasi-kontinuierlichen Prozess zu finden [Montigel 1996].

Beispiel aus der Streckenbetriebssicherung. Abbildung 5.5 zeigt die oberste Abstraktionsebene der Beschreibung des Unfallpotentials des Betriebes auf einer Eisenbahnstrecke. Diese Ebene beschreibt lediglich die möglichen Unfallarten die sich aus den gefährlichen Situationen des Eisenbahnbetriebes im Sinne der Gefahrenanalyse ergeben. Da jeder Unfallauftritt mit einer Reinitialisierung des Modells verbunden ist, hat der Temporalcharakter der Transition *Accident-removal* eher formale Bedeutung (z.B. exponentialverteilt), die nur zur Auswertung der Unfallhäufigkeit angewendet wird. Diese hängt dann von der Auftrittswahrscheinlichkeit einzelner Unfälle wie folgt ab:

$$H_{Acc} = P(Accident = 1) \cdot \lambda_{Accident-removal} \tag{5.1}$$

Dabei ist die $\lambda_{Accident-removal}$ die Rate der Exponentialtransition *Accident-removal* und die $P(Accident = 1)$ die durch Modellanalyse (Kapitel 6) ermittelte Wahrscheinlichkeit der Belegung des Platzes *Accident* mit einem Token.

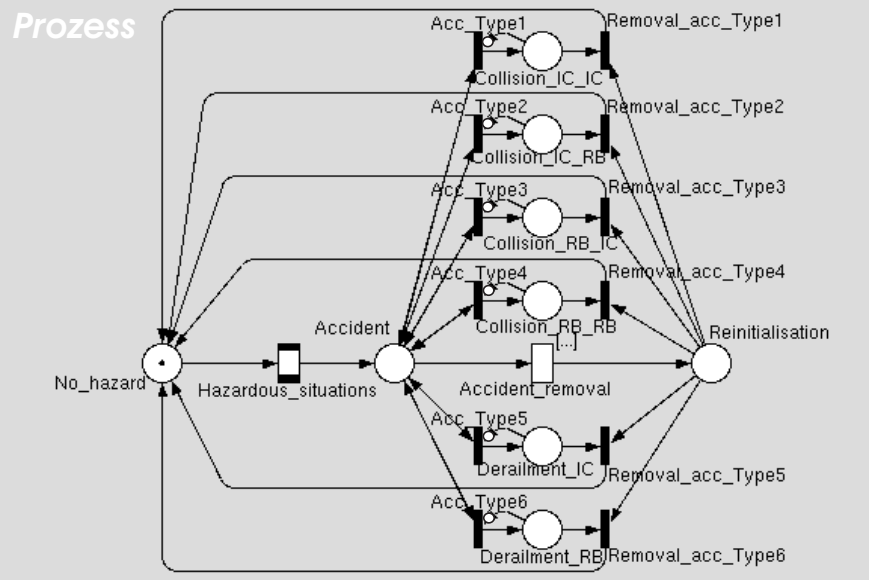

Abbildung 5.5: Modellierung möglicher Unfallarten im betrachteten Beispiel der Streckenbetriebsicherung

Die Dauer der Belegung der einzelnen Unfallartplätze (*Collision*, *Derailment*) ist ebenfalls durch die temporelle Transition *Accident-removal* gegeben. Die dargestellte Unterscheidung der verschiedenen Unfallarten setzt eine Modellierung mit farbigen Token voraus, die die jeweilige Information der Unfallkonkretisierung beinhalten.
Abbildung 5.6 zeigt die Verfeinerung der Instanz *Hazardous-Situations*, die den Zusammenhang zwischen einzelnen gefährlichen Situationen des modellierten Eisenbahnbetriebsprozess es repräsentiert. In dem gegebenen Beispiel wurde die Gefahr des potentiellen Auffahrens zweier Züge (*Collision*) und der Entgleisung (*Derailment*) aufgrund überhöhter Geschwindigkeit jeweils in einem der drei modellierten Streckenabschnitte (*Section*) betrachtet.
Die markierungsabhängigen Gewichte der kausalen Transitionen *Near-miss-event* und *Accident-event* (s. unteren Rand der Abbildung) geben die Wahrscheinlichkeit eines resultierenden Beinaheunfalles oder eines Unfalles an.
Da es sich um Modellierung von seltenen Ereignissen handelt, konnte die Modellkomplexität durch Abgrenzung auf maximal eine gefährliche Situation im betrachteten

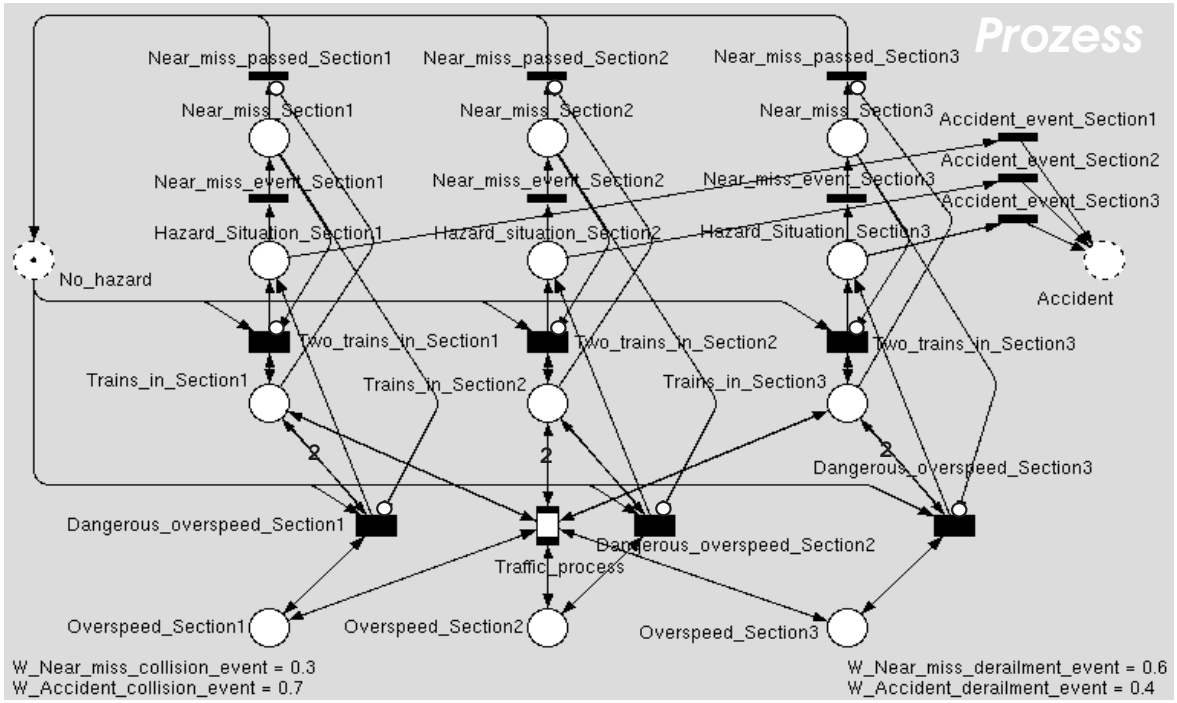

Abbildung 5.6: Modellierung der gefährlichen Situationen im Betriebsprozess und deren Folgen

Beispiel des Betriebsprozesses reduziert werden. Bei Bedarf kann auch ein gleichzeitiger Auftritt dieser Situationen durch Erhöhung der Tokenzahl auf dem Platz *No-hazard* betrachtet werden.
Abbildung 5.7 zeigt die Verfeinerung der Instanz *Traffic-Process* aus Abbildung 5.6, die den eigentlichen Eisenbahnbetrieb auf der Beispielstrecke beschreibt. Als Vereinfachung wurde hier wieder nur einseitiger Zugverkehr betrachtet.

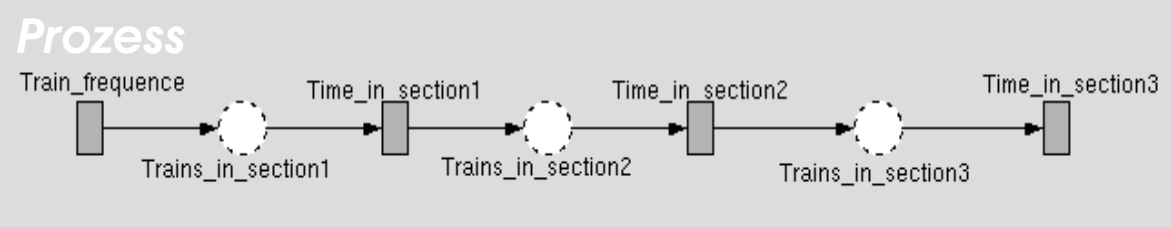

Abbildung 5.7: Modellierung des Betriebsprozesses auf einer eingleisigen Strecke durch drei Abschnitte

Der modellierte Eisenbahnbetriebsprozess ist einerseits von dem geographischen Streckenparameter, andererseits von den betrieblichen Verkehrsparametern der Züge abhängig. Die Einflüsse der Sicherungstechnik sowie der zugseitigen Störungen sind zunächst nicht Gegenstand der Modellierung.
Der betrachtete Streckenteil wurde in drei virtuelle Abschnitte unterteilt. Die Länge der Abschnitte kann theoretisch unendlich klein sein. Die zu wählende Länge entspricht dem minimalen Abstand zwischen zwei fahrenden Zügen und hängt daher von der voraussichtlichen Art der Streckensicherung (z.B. Blocksicherung, Moving Block, relativer Blockabstand) ab.
Die allgemeinen stochastischen Transitionen *Time-in-Section1* bis *Time-in-Section3* bilden die entsprechenden Fahrzeiten der Züge im jeweiligen Streckenabschnitt ab. Die stochastische Verteilung der Temporalparameter dieser Transitionen entspricht der Abschnittslänge und der Variation der Geschwindigkeiten von Zügen, die die betrachtete Strecke befahren. Abbildung 5.8 zeigt die hier angenommene Verteilung der Verweildauer in einem Streckenabschnitt von 1000m Länge für zwei betrachtete Zugtypen (*RB, IC*). Sie könnte entstehen durch Auswertung von statistischen Daten über die Verweildauer betrachteter Züge auf dem modellierten Streckenabschnitt. In diesem Beispiel wird als Approximation die jeweilige minimale Verweildauer (entsprechend maximaler Zuggeschwindigkeit von 120 km/h bzw. 80 km/h) mit einem nach Negativexponentialverteilung variirenden Zeitaufschlag verlängert (mittlerer Zeitaufschlag 5s bzw. 15s)
Die allgemeine stochastische Transition *Train-frequence* entspricht der Zugfolgezeit, deren Streuung vom Tagesfahrplan der betrachteten Züge abhängt und anhand entsprechender statistischer Daten ermittelt werden konnte. Abbildung 5.9 zeigt einen

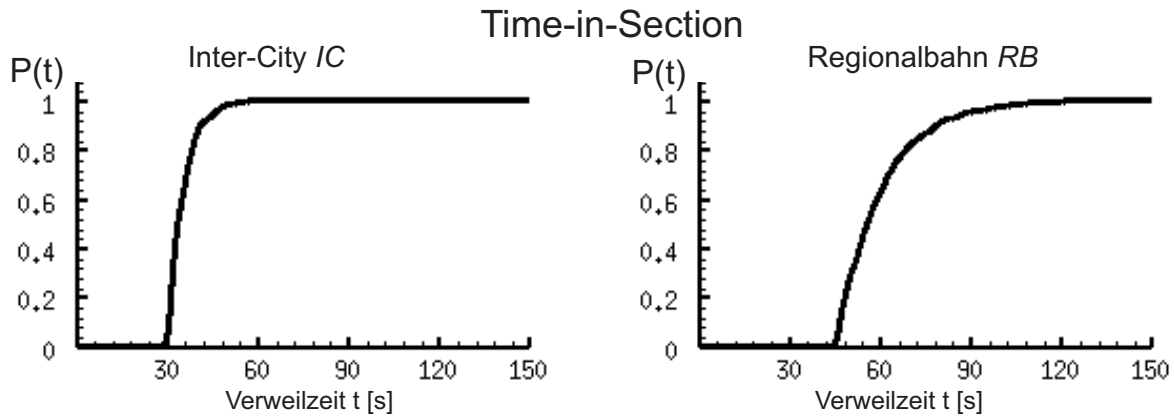

Abbildung 5.8: Angenommene Verteilung der Verweilzeit der Züge in einem Streckenabschnitt der Länge 1000m

möglichen resultierenden Verteilungsverlauf, wobei als minimale Folgezeit 300s (RB) bzw. 1200s (IC) mit jeweiliger Streuung (Negativexponentialverteilung) mit einem Mittelwert von 200s bzw. 400s als Beispiel angenommen wurde.
Die Verwendung von farbigen Petrinetzen konnte dazu genutzt werden, den Detaillierungsgrad der Modellierung zu erhöhen. In diesem Falle entsprechen die Farben der Token den Zugtypen und die Transitionen bilden durch markenabhängige Temporalparameter (Verteilung der Verweildauer) die Fahrzeiten der jeweiligen Züge ab.

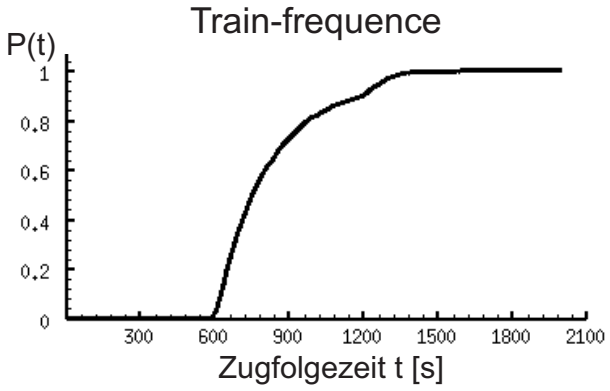

Abbildung 5.9: Angenommene Verteilung der Zugfolgezeit bei zwei Zügen

Eine solche Modellierung des Betriebes auf der betrachteten Strecke ermöglicht, das sich aus dem Fahrplan ergebende Betriebsverhalten zu beschreiben und dessen Bezug zum unerwünschten Betriebsereignis *Kollision* abzubilden. Unter der Voraussetzung keiner zug- sowie streckenseitigen Störungen ist kein Potenzial für ein zweites uner-

wünschtes Ereignis *Entgleisung* in dieser Phase der Modellbildung anzunehmen (die Plätze *Overspeed-Section1* bis *Overspeed-Section2* wurden in die Verfeinerung des Betriebsprozesses (Abb. 5.7) nicht aufgenommen).

5.3.2 Beschreibung der Unfallfolgen

Um das sich aus dem Eisenbahnbetrieb ergebende Risiko auszuwerten, ist es notwendig, den Bezug der identifizierten unerwünschten betrieblichen Ereignisse (Unfälle) zu deren potentiellen Folgen zu beschreiben. Im Rahmen einer solchen Analyse sind alle möglichen Folgen aller Arten unerwünschter betrieblicher Ereignisse zu untersuchen. Neben der Unfallart spielt dabei die aktuelle Betriebslage eine wichtige Rolle, in der das unerwünschte Ereignis eingetreten ist. Aus Sicht der aktuellen Betriebslage sind alle relevanten Bedingungen des Betriebes zu berücksichtigen, die auf das Ausmaß der Unfallfolgen Einfluss haben können [Zahradník et al. 2004]. Die Kombination der Unfallart (U) mit der Betriebslage (B) ergibt eine Unfallsituation (S).

$$S \in U \times B \tag{5.2}$$

Als Größe des Schadensausmaßes wird durch die Norm EN 50 126 das individuelle persönliche Risiko vorgegeben (s. Unterkapitel 2.1). Daher ist es notwendig für jedes unerwünschte Ereignis das Fatalitätspotential einer beteiligten Person (Fahrgast, Angestellter, etc.) zu bewerten. Die weiteren persönlichen Schäden (schwere oder leichte Verletzungen) sind mit entsprechenden Faktoren auf eine so genannte Anzahl der *relativen Todesfälle* umzurechnen.

Grundlage zur Bewertung des gesamten individuellen Risikos ist das statistische kollektive Risiko jeder identifizierten Unfallsituation, das mit entsprechender Anzahl der relativen Todesfälle quantifiziert werden kann (relative Todesfälle pro Unfallsituation). Ein Parameter mit einem Einfluss auf das gesamte individuelle Risiko ist im Eisenbahnbetrieb die Anzahl der gefährdeten Personen pro Zeiteinheit, also die mittlere Anzahl der Fahrgäste in dem untersuchten Eisenbahnsystem. Dieser ist meistens für jede Beförderungsart spezifisch und daher ist der Anteil der Beförderungsart an dem Gesamtverkehr zu berücksichtigen. Da jeder Fahrgast pro Zeiteinheit das Verkehrsystem mehrmals benutzen kann, ist die Anzahl der Nutzungen der Beförderungsart pro benutzte Zeiteinheit ein nächster Faktor von Bedeutung bei der Auswertung.

Ziel der Beschreibung der Unfallfolgen ist die Bildung eines parametrierbaren Modells, das für die identifizierten unerwünschten Ereignisse im Betriebsprozess unter Berücksichtigung aller relevanten Unfallsituationen das entsprechende gesamte individuelle Risiko auszuwerten ermöglicht. Dieses Modell könnte als System von Gleichungen abgebildet werden.

Eine Alternative zu einer solchen Beschreibung der Unfallfolgen bietet die Verwendung von kausalen Petrinetzen, deren Transitionen mit mathematischen Operationen assoziiert werden können. Ein einfaches Beispiel einer Auswertung des individuellen Risikos einer Unfallsituation, in der nur eine Beförderungsart involviert ist (Zugart1), zeigt Abbildung 5.10.

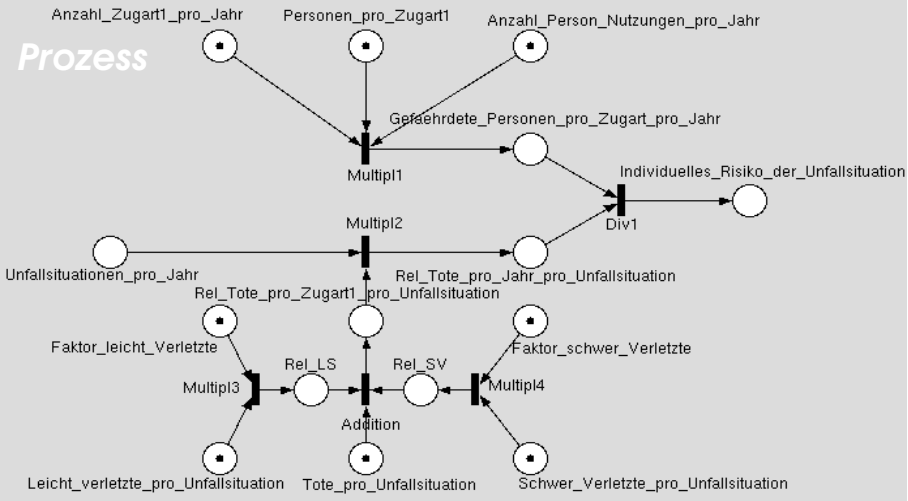

Abbildung 5.10: Beispiel einer Modellierung der Unfallfolgen mit kausalen Petrinetzen

Die Auftrittshäufigkeit der identifizierten Unfallsituationen pro Zeiteinheit (die leeren Eingangsplätze auf der linken Seite der Abb. 5.10) wird durch die Analyse des zu bildenden Modells im Sinne der *PROFUND*-Methode ermittelt. Das gesamte individuelle Risiko des betrachteten Eisenbahnsystems ergibt sich dann aus der Summe:

$$R_{ind} = \sum_{i=1}^{N} R_i \tag{5.3}$$

wobei die R_i die einzelnen unabhängigen Beiträge des individuellen Risikos darstellen. Mit ähnlicher Darstellungsart zeigt Abbildung 5.11 die mögliche Berechnung des individuellen Risikos der Fahrgäste zweier Zugarten (eine Regionalbahn *RB* und ein InterCity *IC*), die auf einer nur in eine Richtung befahrenen Strecke verkehren.
Als Unfallart wurde hier also lediglich eine Kollision durch Auffahren zweier Züge betrachtet. Die Transitionen repräsentieren die prinzipiellen rechnerischen Operationen, die mit einer Marke belegten Plätze die notwendigen betriebsbezogenen Daten aus der Statistik, die leeren Plätze stehen für die Rechenergebnisse. Die leeren Eingangsplätze auf der linken Seite der Abbildung stellen wieder die Schnittstelle dar, die mit den Ergebnissen der Analyse des Modells des Verkehrsprozesses zu parametrieren ist (s. Kapitel 6).

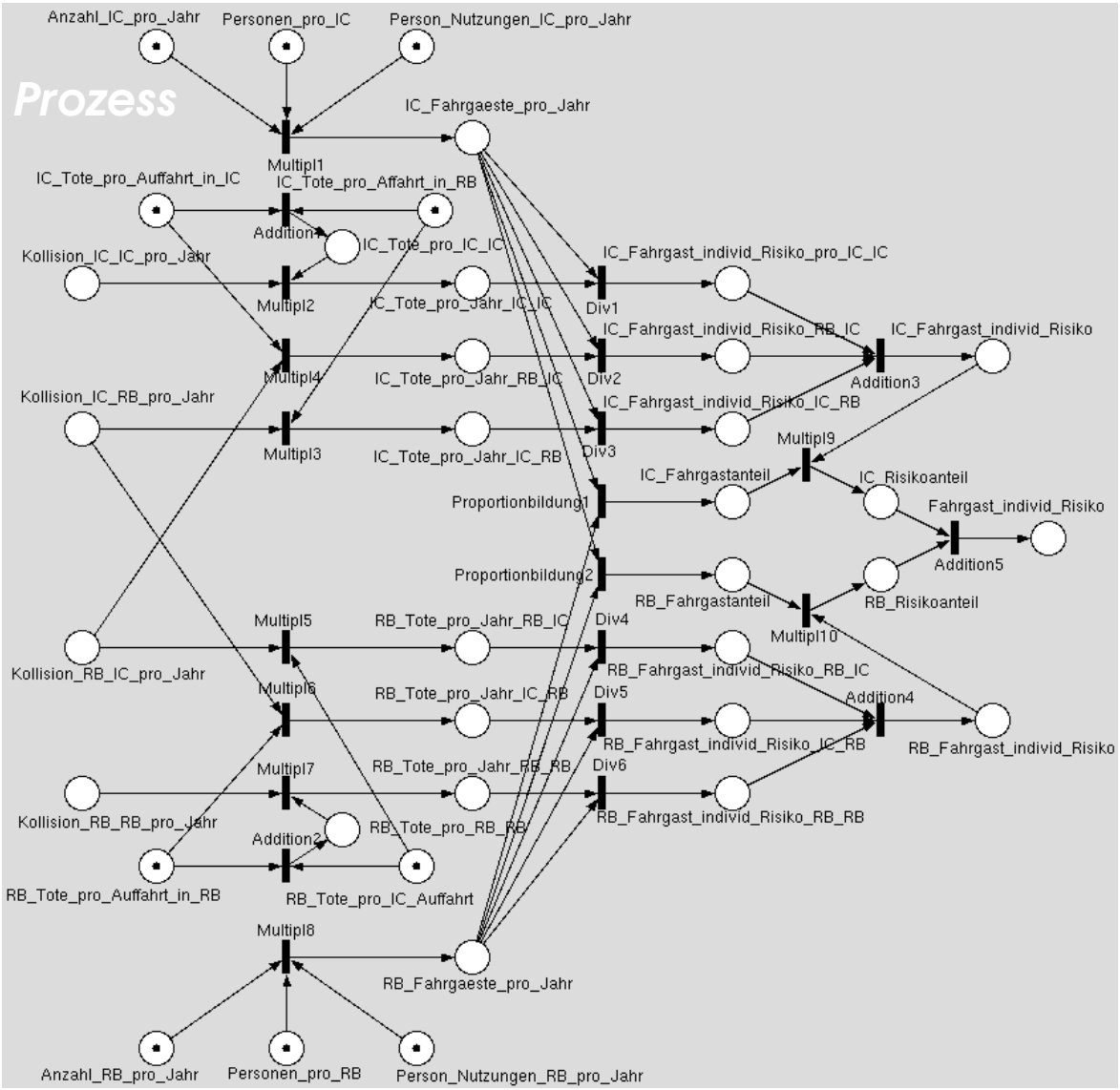

Abbildung 5.11: Modellierung der Unfallfolgen für das Beispiel aus der Streckensicherung

Der gewählte Detaillierungsgrad der Modellierung erlaubt einerseits das individuelle Risiko der Fahrgäste der einzelnen Zuggattungen (*RB* und *IC*) zu unterscheiden, andererseits die vier möglichen Unfallsituationen (*IC-IC*: Auffahren eines *IC* in einen anderen *IC*, *IC-RB*: Auffahren eines *IC* in eine *RB*, usw.) zu berücksichtigen. Durch Integration weiterer Ergebnisse der Analyse des Modells des Betriebsprozesses (z.B. Häufigkeit der Zugstörungen mit einem Halt) kann die Art der Kollision weiter detailliert herunterbrochen und weitere Aspekte des Schadenausmaßes betrachtet werden (z.B. Vergrößerung des Schadensausmaßes bei einer Kollision mit einem haltenden Zug).
Die Beziehungen des Verkehrs und der unerwünschten betrieblichen Ereignisse wurden im Rahmen der Modellierung des Verkehrsprozesses (s. Unterkap. 5.3.1) kausal und quantitativ beschrieben. Abhängig vom Detaillierungsgrad der Beschreibung kann die Modellierung dazu genutzt werden, die unerwünschten Ereignisse nach der jeweiligen Betriebslage weiter zu unterscheiden.
Die Modellierung des Betriebsprozesses selbst berücksichtigt bereits die Dauer, welche die beteiligten Personen dem betrieblichen Risiko ausgesetzt sind. Aus diesem Grund braucht sie in die Modellierung der Unfallfolgen nicht zusätzlich explizit integriert zu werden.

5.4 Beschreibung der Systemfunktionalität

5.4.1 Modellbildung - Systemfunktionalität

Funktionalität im Eisenbahnbereich

Der Eisenbahnprozess kann in den meisten Fällen nur unter Berücksichtigung der Funktionalität der Betriebssteuerung beschrieben werden. Diese reduziert einerseits das Auftreten der unerwünschten Betriebsereignisse, andererseits bringt deren eigene Verlässlichkeitsbetrachtung eine Reihe zusätzlicher Faktoren mit sich, die bei der Beschreibung des Verhalten in Betracht zu ziehen sind.
Aus Sicht der Beanspruchungsdauer werden im Eisenbahnbereich die folgenden zwei Arten Systemfunktionen unterschieden:

- *Funktion auf Aufforderung* ist eine Funktion, die zu bestimmten Zeitpunkten für eine bestimmte Zeitdauer im Eisenbahnprozess zum Einsatz kommt. Ein Ausfall dieser Funktion kann auf den Eisenbahnbetrieb nur während dieser Zeit Auswirkungen haben.

- *Funktion im Dauereinsatz* ist dagegen eine Funktion, die durch den Eisenbahnbetrieb kontinuierlich beansprucht wird. Ein Ausfall dieser Funktion kann im Eisenbahnprozess unmittelbare Auswirkungen haben.

Prinzipiell kann jede Funktion im Dauereinsatz (z.B. bei einem hohen Detaillierungsgrad) durch unendlich limitierende Verkürzung der Zeit zwischen den Anforderungen auch als Funktion auf Aufforderung beschrieben werden. Andererseits kann für eine sehr grobe Beschreibung die Auffassung der meisten Systemfunktionen auch als Funktion im Dauereinsatz angenommen werden.

Generelle Modellierung des funktionalen Verhaltens

Methodische Grundlage für die Modellbildung ist der funktions-orientierte Modellierungsansatz von [Meyer zu Hörste 2003], der auf einer bekannten Verhaltensweise und Struktur der Systemfunktionen basiert.
Basis für die Modellierung bildet die Hauptaufgabe des Systems, die in der Vermeidung der unerwünschten grundsätzlichen Betriebsereignisse liegt. Die erste Ergänzung des Betriebsprozesses sollte daher die Funktionen *Vermeidung der Kollision* und *Vermeidung der Entgleisung* der Züge sein.
Die Modellierung dieser Basisfunktionen ist meistens zu abstrakt und die funktionale Modellierung verlangt meistens einen weiteren Grad der Konkretisierung. Deswegen beinhaltet die Ergänzung des Betriebsprozesses die Modellierung der Funktionen, die es ermöglichen, diese Basisfunktionalität zu erreichen.
Ähnlich wie in der Phase der Modellierung des reinen Betriebsprozesses ist auch bei der Abbildung der Systemfunktionalität auf die Ergebnisse der Gefahrenanalyse zurückzugreifen. Einerseits gibt die Gefahrenanalyse das Abstraktionsniveau der funktionalen Modellierung vor. Andererseits bestimmt die Gefahrenanalyse im Wesentlichen den modellierten Systemfunktionsumfang, da insbesondere die Systemfunktionen zu modellieren sind, die in direktem Bezug zu unerwünschten Betriebsereignissen stehen. Der Funktionsumfang steht auch in einem engen Bezug mit der Art der technischen Realisierung, die der Betreiber vorsieht, um die Basisfunktionalität des Systems zu erfüllen. Neben den Funktionen aus der Gefahrenanalyse sind auch weitere Funktionen Gegenstand der Modellierung, die oft keine Sicherheitsrelevanz aufweisen. Deren Integration ist meist notwendig, um den Ablauf des Betriebsprozesses vollständig abbilden zu können. Andererseits können dadurch innerhalb des Modells auch weitere Aspekte der Verlässlichkeit (z.B. Verfügbarkeit, Instandhaltbarkeit) beschrieben werden.
Die Steuerung des Eisenbahnbetriebes erfolgt durch das Zusammenwirken mehrerer ELSS. Die Funktionalität dieser Systeme befindet sich je nach realisiertem Betriebsverfahren einerseits entlang der Strecke (z.B. Streckenblock, Fahrstraßensicherung,..), andererseits ist sie an den Eisenbahnfahrzeugen (z.B. Geschwindigkeitsregelung/-überwachung usw.) implementiert. Wie schon bereits erwähnt, kann als Grundlage zur funktionalen Modellierung die Klassifikation der Funktionen des Eisenbahnsystems durch AEIF [AEIF 2002] herangezogen werden. Eine ebenso vollständige formale Beschrei-

bung der Funktionen mit farbigen Petrinetzen (CPN) wird in [Meyer zu Hörste 2003] dargestellt.
Die methodische Basis der funktionalen Modellierung bildet das Funktions-Ressourcen-Modell [Schnieder und Bikker 1998] [VDI3682 2002]. Die Voraussetzung der Anwendung dieses Ansatzes ist, dass die Funktionalität des ELSS in Einzelfunktionen zerlegbar ist, wobei jede Einzelfunktion des Systems als Reaktion auf eine Auslösung (Eingang) unter Erfüllung bestimmter funktionaler Bedingungen gesehen werden kann. Außerdem muss es möglich sein, jede Systemfunktion einer bzw. mehreren betrieblichen Ressourcen zuzuordnen, die der Betreiber zur Steuerung des Betriebsverhaltens vorsieht. Die Verfügbarkeit der notwendigen (bzw. aller notwendigen) Ressourcen ist eine Voraussetzung zu einem korrekten Einfluss der Systemfunktion auf den Betriebsprozess bzw. auf die anderen Funktionen.
Abbildung 5.12 zeigt den grundlegenden Baustein funktionaler Petrinetzmodellierung für eine Funktion auf Aufforderung, wobei die Funktion als Transition und die funktionale Ressource, die funktionalen Bedingungen sowie die Funktionsein- und -ausgänge als Plätze dargestellt sind.

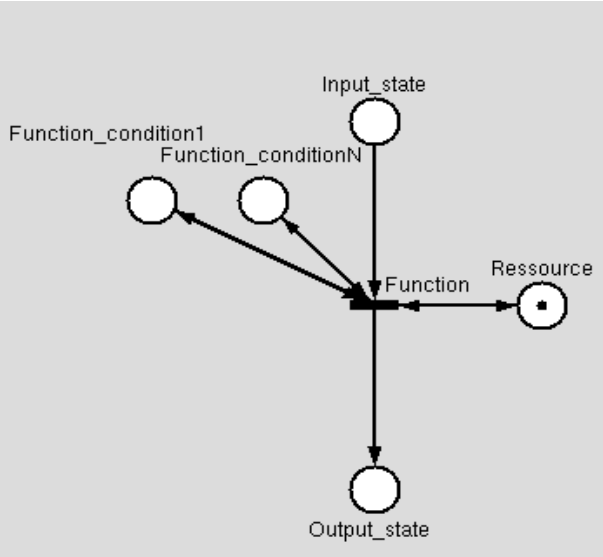

Abbildung 5.12: Elementare Modellierung einer Systemfunktion auf Aufforderung

Da es sich bei der Modellierung des funktionalen Verhaltens um eine deterministische Beschreibung handelt, wird die eigene Systemfunktion entweder mit einer kausalen oder deterministisch temporalen Transition abgebildet. Die Erfüllung der Eingangsbedingungen entscheidet darüber, wann die Systemfunktion seitens des Betriebsprozesses angefordert wird.

Im Falle einer hohen Häufigkeit der Inanspruchnahme einer Funktion auf Anforderung (z.B. periodische Aufrufe) oder bei einem niedrigeren Detaillierungsgrad der Beschreibung (z.B. für Funktionen außerhalb des Hauptinteresses der Modellierung, wie z.B. Funktionalität der Nachbarsysteme) kann diese als eine Funktion im Dauereinsatz angenommen werden. Bei solcher Funktion reduziert sich die dynamische Modellierung (Funktion als Transition) auf eine statische, indem nur der Platz der Funktionsressource beibehalten wird. Dieser kann direkt mit dem Betriebsprozess gekoppelt werden bzw. bildet selbst eine Bedingung zur Durchführung anderer Funktionen auf Anforderung.

Beispiele funktionaler Modellierung

Beispiel aus der Streckenbetriebsicherung. Abbildung 5.13 zeigt ein Beispiel der Modellierung einer einfachen Fahrwegsicherung (Train Route Control), die zur Abbildung der Funktionalität der Streckenblocksicherung im Betriebsprozess angewendet werden kann. Da diese Funktionalität nur bei einer Durchfahrt eines Zuges in Anspruch genommen wird, sind in dem Modell die Funktionen auf Anforderung verwendet. Dieses Modell besteht aus zwei elementaren Funktionen: Zugerkennung (*Detecting-train-in-block* und Erkennung der Blockfreiheit *Detecting-block-free*). Die funktionale Eingangsbedingung bildet der belegte bzw. der nicht belegte Block (jeweilige Plätze *Trains-in-section1* bis *Trains-in-Section3* markiert bzw. nicht markiert) im Betriebsprozess. Als Ressource für die beiden elementaren Funktionen wird die Verfügbarkeit der Funktion der Fahrwegsicherung (*Train-Route-Control*) vorausgesetzt.

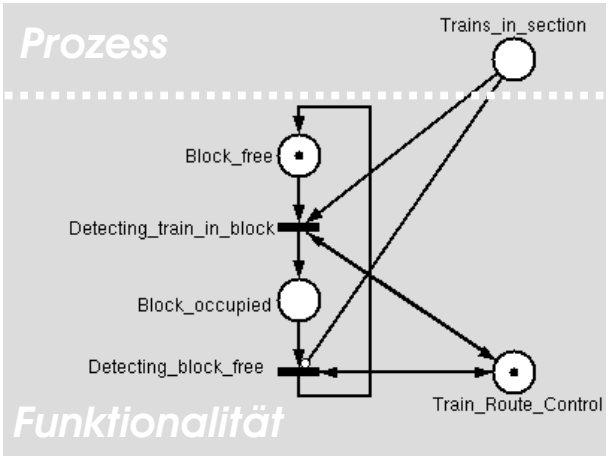

Abbildung 5.13: Elementare Modellierung einer Systemfunktion am Beispiel der Fahrwegsicherung

In dem betrachteten Beispiel der Streckenbetriebsicherung gehört zu der funktionalen Modellierung einerseits die streckenseitige Funktionalität, die Fahrwegsicherung, z. B.

durch einen automatischen Streckenblock, andererseits die fahrzeugseitige Funktionalität, die Fahrzeugsicherung (Train Protection), (s. Funktionsklassifizierung in Abb. 5.2). Die Integration der Funktion der Fahrwegsicherung (Abb.5.13) mit dem Betriebsprozess der eingleisigen Strecke (Abb. 5.7) zeigt Abbildung 5.14. Die Verfeinerung der Instanz Function-Train-Route-Control befindet sich in Abbildung 5.15. Jedem Blockabschnitt ist eine eigene Funktion der Zugerkennung und Blockfreimeldung zugewiesen, wobei alle Funktionen die Ressource der Fahrwegsicherung (Platz *Train-Route-Control*) verwenden.

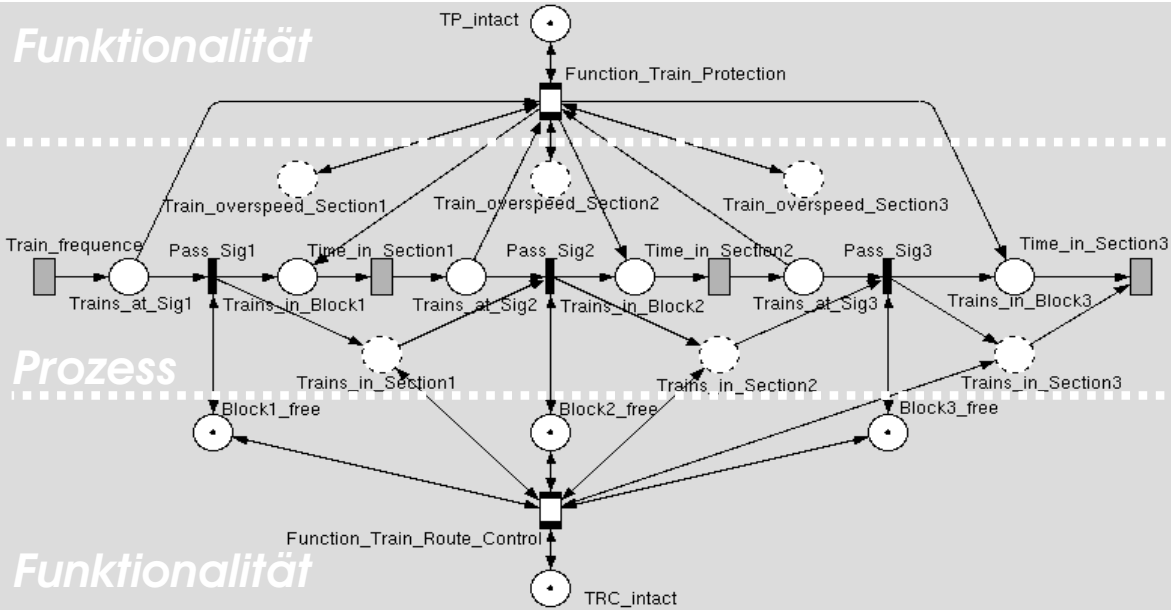

Abbildung 5.14: Betriebsprozess einer eingleisigen Strecke und seine Erweiterung um die Funktionalität der Fahrweg- und Fahrzeugsicherung

Durch die Funktionalität der Fahrwegsicherung wird der Betriebsprozess auf der Beispielstrecke beeinflusst, und deshalb ist es auch notwendig seine Modellierung zu erweitern. Einerseits sind es die Signale, die die Weiterfahrt eines Zuges nur in einen freien Folgeblock erlauben (Abfragekante von dem jeweiligen Platz *Block-free* zu der jeweiligen Transition *Pass-Sig*). Andererseits ist es die mögliche Verlängerung der Fahrzeit des Zuges im Block durch einen Halt vor einem Halt zeigenden Signal (modelliert jeweils durch einen zusätzlichen Platz *Trains-at-Sig1* bis *Trains-at-Sig3*).
Die Annahme fehlerfreier Funktionsfähigkeit der Fahrwegsicherung sorgt in dem Modell für kollisionsfreien Betrieb, was durch Modellanalyse verifiziert werden kann, (s. Kap. 6). Neben der streckenseitigen Funktionalität wird der Betrieb auch durch zugseitige Funktionalität durch die Fahzeugsicherung beeinflusst. Die Fahrzeugsicherung, die die

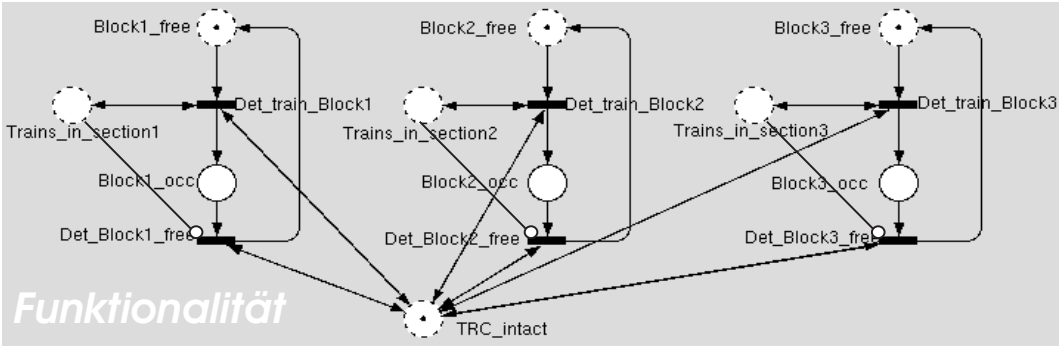

Abbildung 5.15: Funktionale Modellierung der Fahrwegsicherung auf der Beispielstrecke

Zuggeschwindigkeitsüberwachung umfasst, wird während der ganzen Fahrt der Züge über die modellierten Streckenblöcke beansprucht und kann daher als Funktion im Dauereinsatz modelliert werden (modelliert durch einen belegten Platz *TP-intact*). Durch die Annahme seiner Fehlerfreiheit wird aber das modellierte Betriebsverhalten nicht weiter beeinflusst (die Züge respektieren die Streckengeschwindigkeit sowie die Signale), und das Modell des Betriebsprozesses braucht in diesem Falle nicht verfeinert werden.

Beispiel aus der Bahnhofssicherung. Abbildung 5.16 zeigt ein anderes Modellierungsbeispiel, ein Modell der Funktion "Stellung einer Zugfahrtstraße" auf der Basis der Klassifizierung nach [Meyer zu Hörste 2003]. Diese kann beispielhaft in Einzelfunktionen wie Empfang der Aufforderung (*Obtaining-request*), Fahrstraße stellen und verschließen (*Setting-route*), Einfahrt in die Fahrstrasse sperren (*Stopping-entrance*) und Fahrstraße auflösen (*Setting-route-free*) zerlegt werden. Das Modell der Funktion entsteht in diesem Fall durch Aufreihung der im Sinne der Abbildung 5.12 modellierten Einzelfunktionen. Eine vorzeitige Rücknahme der Stellung der Fahrstraße repräsentiert die Transition *Cancelling-route-setting*. Da für die ordnungsgemäße Durchführung der Funktionen die Überprüfung und die korrekte Reihenfolge der Eingangsbedingungen wichtig ist, wurden ausschließlich die kausalen Transitionen verwendet.

Als funktionale Ressource aller Unterfunktionen der Stellung der Fahrstraße wurde die Fahrwegsicherung identifiziert (der Platz *Train-Route-Control*). Die Modellierung des Versagens der Systemfunktionalität ist Bestandteil der dritten Phase der Modellbildung.

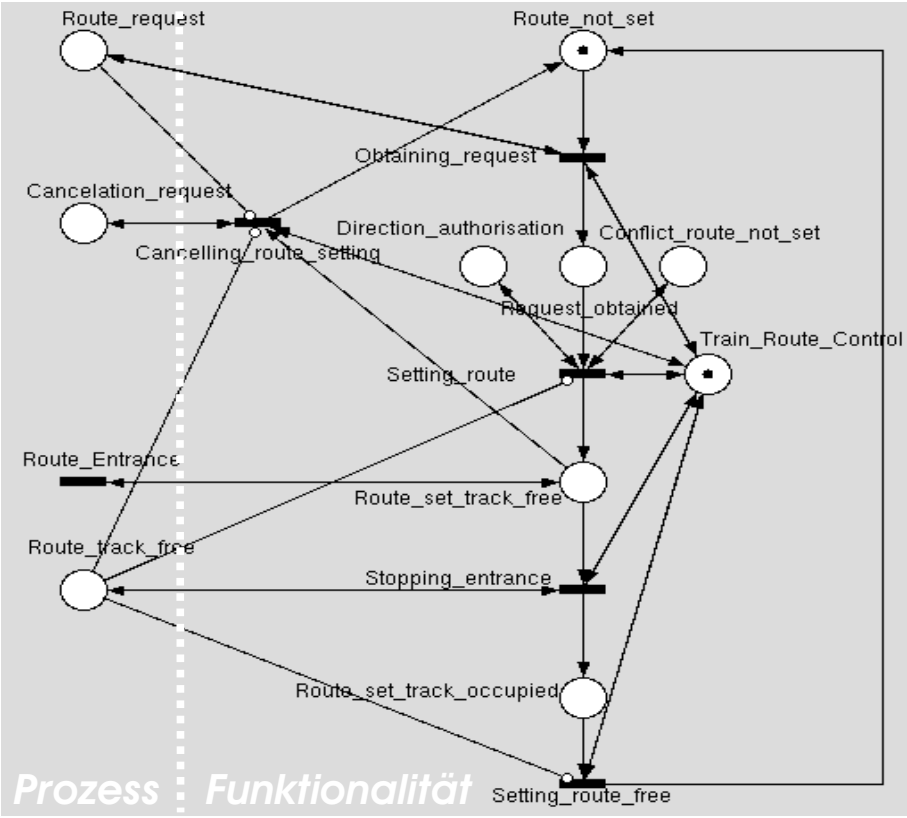

Abbildung 5.16: Modellierung der Funktionalität der Stellung einer Zugfahrtstraße

5.4.2 Modellbildung - Systemfunktionsverlässlichkeit

Verlässlichkeitsverhalten im Eisenbahnbereich

Basierend auf der Gefahrenanalyse ist es möglich die modellierten Systemfunktionen zu identifizieren, deren Versagen den Auftritt von unerwünschten Betriebsereignissen verursachen kann. Die *PROFUND*-Methode unterscheidet eindeutig zwischen dem Verkehrsprozess und der Systemfunktionalität. Diese Unterteilung ermöglicht im Rahmen der Verlässlichkeitsbetrachtung der Funktionsressourcen sehr einfach die Systemfunktionalität zu erweitern, ohne das Modell des Verkehrsprozesses modifizieren zu müssen. Für die Aufgabe der Sicherheitsbetrachtung sind die folgenden grundlegenden Verlässlichkeitszustände der funktionalen Ressource relevant:

- Betriebszustand *(intact state)* - ist der Zustand der Ressource, in dem sie in der Lage ist, die volle vorgesehene Funktion dem Eisenbahnbetrieb zu gewährleisten.
- Fail-Safe-Zustand *(fail-safe state)* - ist ein Fehlerzustand der Ressource, in dem dem Eisenbahnbetrieb nur eine beschränkte Funktionalität zur Verfügung steht, ein Auftritt eines Gefahrzustandes ist jedoch ausgeschlossen.
- Hazardzustand *(hazard state)* - ist ein Fehlerzustand in dem die Ressource für den Eisenbahnbetrieb eine potentielle Gefahr darstellt.

Im Falle von mehreren unterschiedlichen möglichen Fehlerzuständen der Ressource ist der meist-betriebshindernde Fail-Safe-Zustand bzw. der Gefahrzustand mit größter potentieller Gefahr zu betrachten. Sollte diese Annahme zu großen sicherheitsrelevanten Ungenauigkeiten führen, ist eine entsprechende Verfeinerung des Verlässlichkeitsverhaltens vorzunehmen.
Die Unterscheidung der zwei Arten der Fehlerzustände (Fail-safe- und Hazardzustand) führt auch zu zwei Typen der Systemfunktionen aus der Sicht der Verlässlichkeit. Jede Funktion, deren Ressource einen Hazardzustand einnehmen kann, ist für den Eisenbahnbetrieb eine *sicherheitsrelevante Funktion* und alle anderen, deren Ressource sich nur in einem Fail-Safe Zustand befinden können, sind aus der Sicht der Verlässlichkeit *nicht-sicherheitsunrelevante Funktionen*.
Aus Sicht der Aktivierung ist es möglich, die *sicherheitrelevanten Funktionen* wie folgt zu unterscheiden:

- *Hazard-aktive Funktion* ist eine Funktion, deren fehlerhafte *Aktivierung* aufgrund des Hazardzustandes ihrer Ressource in einen Zustand führt, der für den Eisenbahnbetrieb eine potentielle Gefahr darstellt (z.B. Einschaltung eines permissiven Signals),

- *Hazard-passive Funktion* ist eine Funktion, deren fehlerhaftes *Ausbleiben* (nicht Aktivierung) aufgrund des Hazardzustands ihre Ressource in einen Zustand führt, der für den Eisenbahnbetrieb eine potentielle Gefahr darstellt .

Im Rahmen der Beschreibung des Verlässlichkeitsverhaltens sind nicht nur alle Ausfallzustände sondern auch alle möglichen Hazardverlaufs- und -erkennungsarten der Ressource zu betrachten, wobei alle möglichen Folgen der grundlegenden Verlässlichkeitszustände sowie die Arten der Zustandsübergänge zu berücksichtigen sind. Aus der Sicht des Eisenbahnbereiches konnten die sechs typischen Hazardverlaufsarten identifiziert werden. Die zeitliche Abfolge der einzelnen Verlässlichkeitszustände mit charakteristischen Ereignissen und Zeitdauern zeigt Abbildung 5.17.

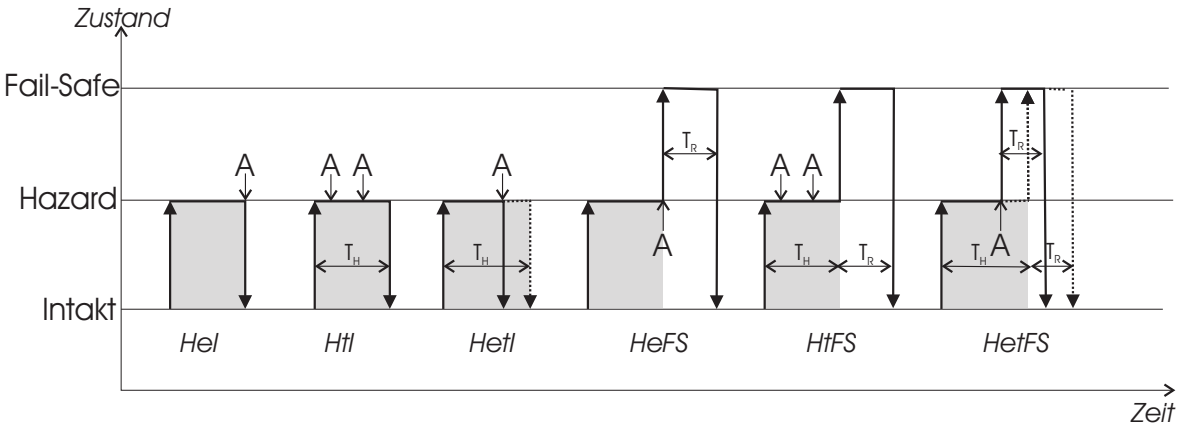

Abbildung 5.17: Die grundsätzlichen Arten der zeitlichen Hazardzustandsverläufe, die graue Hinterlegung entspricht der längsten Dauer des Funktionshazards

Es handelt sich um die folgenden einzelnen Arten von Hazardverläufen:

- Hazard - Aufforderung - Intakt (HeI) - nach dem Auftritt des Hazardzustandes wird bei der nächsten Aufforderung die Funktion fehlerhaft durchgeführt, diese Durchführung sorgt aber zur Hazarderkennung und zum anschließenden Intaktzustand der Ressource. Ohne eine Aufforderung der Funktion dauert der Hazardzustand der Ressource unbegrenzt an.

- Hazard - Zeitdauer - Intakt (HtI) - der Hazardzustand tritt für eine Zeitdauer (T_H - stochastisch oder deterministisch) ein, innerhalb dieser Zeit werden alle Aufforderungen an die Funktion fehlerhaft durchgeführt. Nach Ablauf der Zeitdauer wird der Intaktzustand wiedererreicht ohne den vorhergehenden Hazard zu erkennen.

- Hazard - Aufforderung/Zeitdauer - Intakt (*HetI*) - der Hazardzustand tritt für eine Zeitdauer T_H (stochastisch oder deterministisch) ein, wobei die erste Aufforderung der Funktion zur Hazarderkennung und zum anschließenden Intaktzustand der Ressource führt. Nach Ablauf der Zeitdauer ohne die Inanspruchnahme der Funktion wird der Intaktzustand wiedererreicht ohne den vorhergehenden Hazard zu erkennen.

- Hazard - Aufforderung - Fail-Safe (*HeFS*) - nach Auftritt des Hazardzustandes wird bei der nächsten Aufforderung die Funktion fehlerhaft durchgeführt, diese Durchführung führt aber zur Hazarderkennung und zum anschliessenden Fail-Safe Zustand der Ressource. Ohne eine Aufforderung der Funktion dauert der Hazardzustand der Ressource unbegrenzt. Nach einer Reparaturzeit (T_R - stochastisch oder deterministisch) wird die Ressource in einen intakten Zustand gebracht.

- Hazard - Zeitdauer - Fail-Safe (*HtFS*) - der Hazardzustand tritt für eine Zeitdauer (T_H - stochastisch oder deterministisch) ein, innerhalb dieser Zeit werden alle Aufforderungen an die Funktion fehlerhaft durchgeführt. Nach Ablauf der Zeitdauer T_H wird der Hazardzustand erkannt und in einen Fail-Safe-Zustand überführt. Nach einer Reparaturzeit T_R wird die Ressource in einen intakten Zustand gebracht.

- Hazard - Aufforderung/Zeitdauer - Fail-Safe (*HetFS*) - der Hazardzustand tritt für eine Zeitdauer (T_H stochastisch oder deterministisch) ein, wobei die erste Aufforderung der Funktion zur Hazarderkennung und zum anschließenden Fail-Safe-Zustand der Ressource führt. Nach Ablauf der Zeitdauer ohne die Inanspruchnahme der Funktion wird der Hazard erkannt und der Fail-Safe-Zustand erreicht. Nach einer Reparaturzeit T_R wird die Ressource in einen intakten Zustand gebracht.

Die genannten Hazardverlaufsarten betreffen die funktionalen Ressourcen, die keine relevante Beziehung zu anderen Ressourcen aufweisen, so dass ihr Verlässlichkeitsverhalten als unabhängig betrachtet werden kann. In der Praxis wird aber oft festgestellt, dass ein Ressourcenausfall durch externe Ereignisse (z.B. im Betriebsprozess) oder durch Ausfälle anderer funktionaler Ressourcen (z.B. gemeinsame Ausfallursache) bedingt ist. Andererseits werden oft mehrere Ausfallzustände gleichzeitig erkannt bzw. behoben (z.B. durch Funktion einer Fehlerdiagnostik, durch einen Wartungseingriff, etc.). Da eine Berücksichtigung solcher Ereignisse nur durch stochastische Attributierung des Verlässlichkeitsverhaltens der Ressource oft zu unerwünschten Ungenauigkeiten der Beschreibung führt, wird angenommen, dass jeder temporale Übergang zwischen zwei Verlässlichkeitszuständen auch durch eine externe Bedingung vorzeitig

ausgelöst werden kann. Dieses führt auch zur Ergänzung der Zeitabfolge der genannten Hazardverlaufsarten um den Einfluss der Bedingungen, wie Abbildung 5.18 zeigt.

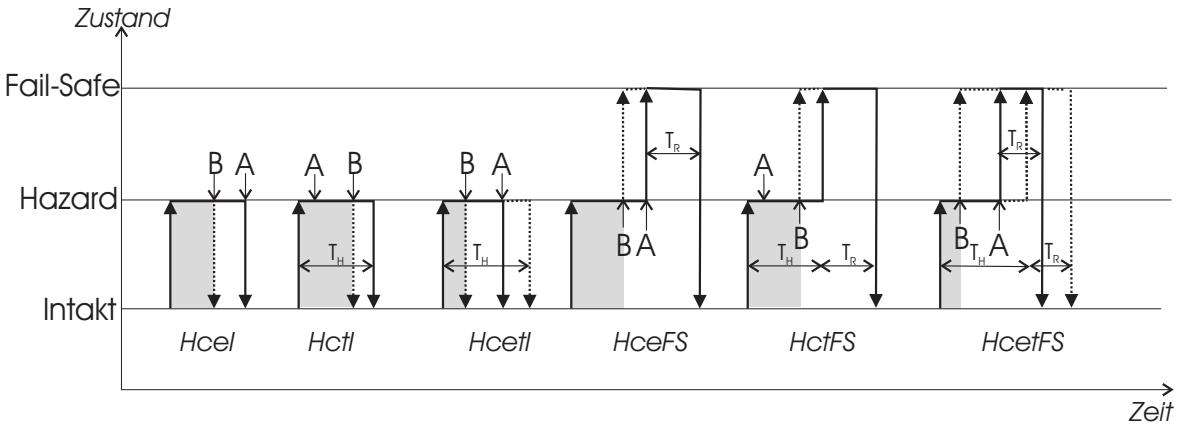

Abbildung 5.18: Die grundsätzlichen Arten der zeitlichen Hazardzustandsverläufe mit Einfluss einer externen Bedingung; die graue Hinterlegung entspricht der durch die Bedingung gekürzten Dauer des Funktionshazards

Generelle Modellierung des Verlässlichkeitsverhaltens

Abbildung 5.19 zeigt die Erweiterung des Funktions-Ressourcen-Modells um das generelle Verlässlichkeitsverhalten. Die einzelnen Verlässlichkeitszustände der Ressource sind mit drei Plätzen (*Ressource-intact*, *Ressource-fail-safe*, *Ressource-hazard*) abgebildet. Die Zustandsübergänge sind durch entsprechende Instanzen repräsentiert; diese bilden sowohl das temporal-stochastische als auch das kausale Verlässlichkeitsverhalten der Ressource ab. Das temporale (selbstbedingte) Verhalten ist durch die stochastische Wahrscheinlichkeitsverteilung des Ausfalles bzw. der Reparatur gegeben. Das kausale (externbedingte) Verhalten tritt nach Erfüllung der Bedingungen außerhalb der Ressource (z.B. externe Erkennung eines Hazardzustandes repräsentiert durch Platz *condition-hazard-to-fail-safe*) ein. Hier ist zu bemerken, dass bei der funktionalen Verlässlichkeitsmodellierung ohne Kenntnis der technischen Funktionsimplementierung ausschließlich funktions-externe Hazarderkennungsarten zu betrachten sind. Die Funktion selbst ist auch als Instanz dargestellt, das heißt die Schaltfähigkeit im Sinne der Petrinetzregel ist erst auf der Verfeinerungsebene eingehalten.
Abbildung 5.20 zeigt eine allgemeine Verfeinerung aller genannten Instanzen aus Abbildung 5.19 für eine hazard-aktive Funktion. Im Falle eines Hazardauftrittes wechselt die hazard-aktive Funktion ihren Zustand (Funktion wird aktiviert) ohne Erfüllung ihrer Aktivierungsbedingungen. Die Verfeinerungen der Instanzen der Übergänge vom

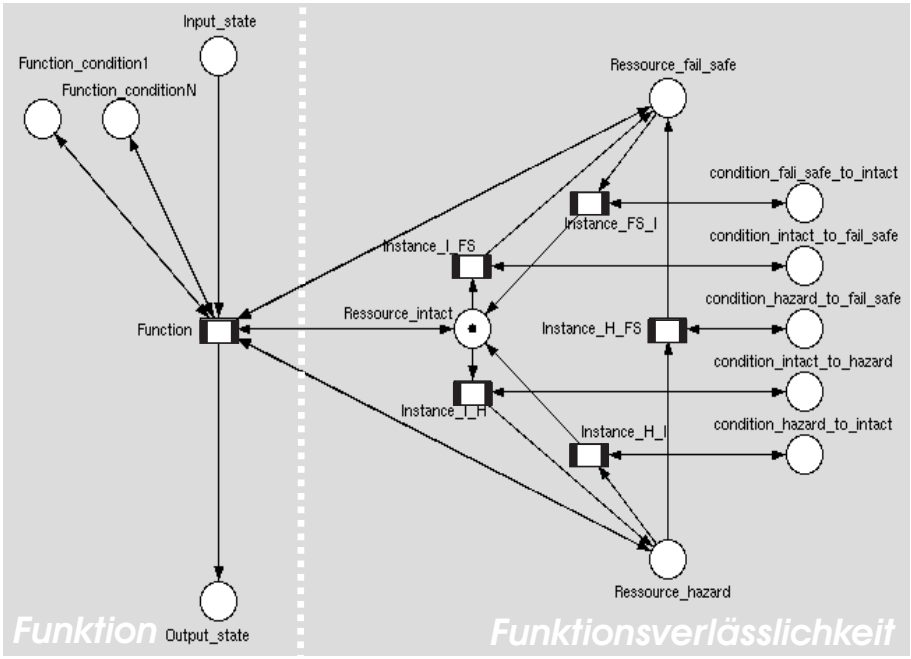

Abbildung 5.19: Generelle Erweiterung einer Funktion um Verlässlichkeitsverhalten

Hazard- zum Intakt- bzw. zum Fail-Safe-Zustand enthalten die Modellierung der sechs grundlegenden Hazardverlaufsarten aus Abbildung 5.17 (modelliert durch die zeitlosen Transitionen *HeI*, *HtI*, *HetI* bzw. *HeFS*, *HtFS*, *HetFS*). Die probabilistische Gewichtung dieser Transitionen gibt die Auftrittswahrscheinlichkeit der jeweiligen Hazardververlaufsart nach dem Auftritt des Hazardzustandes der funktionalen Ressource an.
Der Hazardzustand der Ressource selbst ist mit dem Platz *Ressource-hazard* modelliert. Gleichzeitig wird der Platz Hazard-typ belegt, welcher je nach der Verlaufsart mit einem Zustandsplatz (z.B. *HeI-state*) über die entsprechend gewichtete kausale Transition (hier z.B. *HeI*) verbunden ist. Die Verbindung des Zustandsplatzes mit der entsprechenden kausalen Transition der Instanz der Funktion (*Function-HeI*) bildet die jeweilige gefährliche Durchführung der Funktion ab. In diesem Falle können die funktionalen Eingangsbedingungen völlig ignoriert (wie in Abb. 5.20 dargestellt) oder nur teilweise wahrgenommen werden. Die Zeitdauer des Verbleibens der Funktionsressource in dem Hazardzustand wird mit entsprechenden allgemeinstochastischen temporalen Transitionen (*HetI-time*, *HetI-time*, *HtFS-time*, *HetFS-time*) modelliert. Das vorzeitige Verlassen des Hazardzustandes aufgrund externer Bedingungen entsprechend der Abbildung 5.18 (z.B. durch externe Hazarderkennung) wird jeweils durch die kausalen Transitionen (*HceI*, *HctI*, *HcetI* und *HceFS*, *HctFS*, *HcetFS*) abgebildet. Die externen Bedingungen können auch die anderen temporalen Übergänge vorzeitig

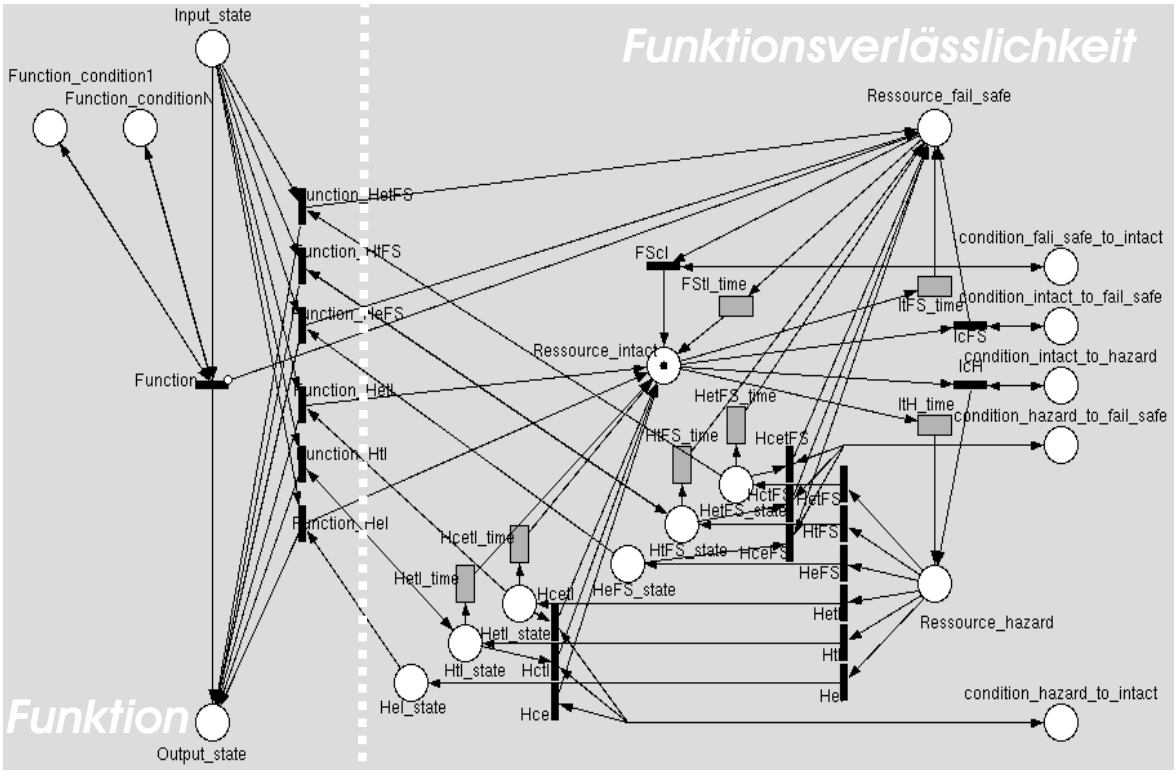

Abbildung 5.20: Generelle Verfeinerung des Verlässlichkeitsverhaltens einer hazard-aktiven Funktion

auslösen, z.B. Modellierung der externen Inbetriebnahme aus dem Fail-Safe-Zustand in den Intakt-Zustand durch die zeitlose Transition *FScI*. Ebenso können das extern bedingte Erreichen des Fail-Safe bzw. des Hazardzustandes durch die Transitionen *IcFS* bzw. *IcH* modelliert werden.
Abbildung 5.21 zeigt die Verfeinerung der Instanzen aus Abbildung 5.19 für eine hazard-passive Funktion. In diesem Falle stellt der Eingangszustand (*Input-State*), der bei der Aufforderung der Funktion nicht verlassen wird, eine Gefahr für den Betrieb dar. Dagegen erzwingt ein Auftritt des Fail-Safe Zustandes der Ressource die Aktivität der Funktion ohne vorliegende Aufforderung. Ein erkennbarer Unterschied gegenüber dem Modell der hazard-passiven Funktion bilden die zwei zusätzlichen Plätze *HeFS-store* und *HeI-store*, deren Zweck es ist, den Auftritt des Aufforderungsereignisses zu erkennen und vorüberläufig zu speichern. Die Ressource erreicht den Folgezustand ihres Hazardzustands (*Ressource-fail-safe* oder *Ressource-intact*) nach dem Ende der ersten Aufforderung (im Sinne der Hazardverlaufsarten aus Abb. 5.17).

Praktische Anwendung der generellen Verlässlichkeitsmodellierung Bei einer praktischen Modellierung kann die Betrachtung von bestimmten Übergängen zwischen den Verlässlichkeitszuständen der Ressource im Falle der hazard-aktiven oder hazard-passiven Funktionen irrelevant sein, z.B. Möglichkeit aller Hazardzustandsverläufe oder bedingter Zustandsübergänge. Daher ist es die Aufgabe des Anwenders anhand der Systemkenntnis nur die relevanten Übergänge im Verlässlichkeitsmodell der Ressource beizubehalten.
Das letztendliche Ziel der funktionalen Verlässlichkeitsmodellierung ist, anhand des resultierenden Risikos im Betriebsprozess die funktionalen Sicherheitsziele zu definieren. Dabei ist es offensichtlich, dass dieses Risiko proportional der Auftrittswahrscheinlichkeit des funktionalen Hazardzustandes ist. Da diese Auftrittswahrscheinlichkeit stark von der Intensität der Hazarderkennungsart (Offenbarungszeit) anhängig ist, ist es für eine korrekte Ermittlung der Sicherheitsziele wichtig, dass bei der funktionalen Modellierung keine system-internen Hazardekennungsarten betrachtet werden, die für die vorgesehenen implementierungsabhängigen Systemlösungen charakteristisch sind. Es sollen nur tatsächliche system-externe Hazarderkennungsmöglichkeiten berücksichigt werden, wobei oft von dem *Worst-Case* Fall auszugehen ist. Eine andere Vorgehensweise könnte zur Unterschätzung der Sicherheitsziele führen. Im Falle keiner sicheren Zeitbegrenzung der Dauer der Hazarderkennung (z.B. nur nach einem Unfall), können die Übergänge aus dem Hazardzustand in der Modellierung (im Sinne des Verlässlichkeitsverhaltens ohne Reparatur) weggelassen werden. Der Hazardzustand wird in diesem Fall nur durch Reinitialisierung des Modells verlassen. Es ist dann Aufgabe der Modellierung der Systemimplementierung, weitere geeignete Hazarderkennungsarten herauszufinden um die höheren funktionalen Sicherheitsziele auch mit Komponen-

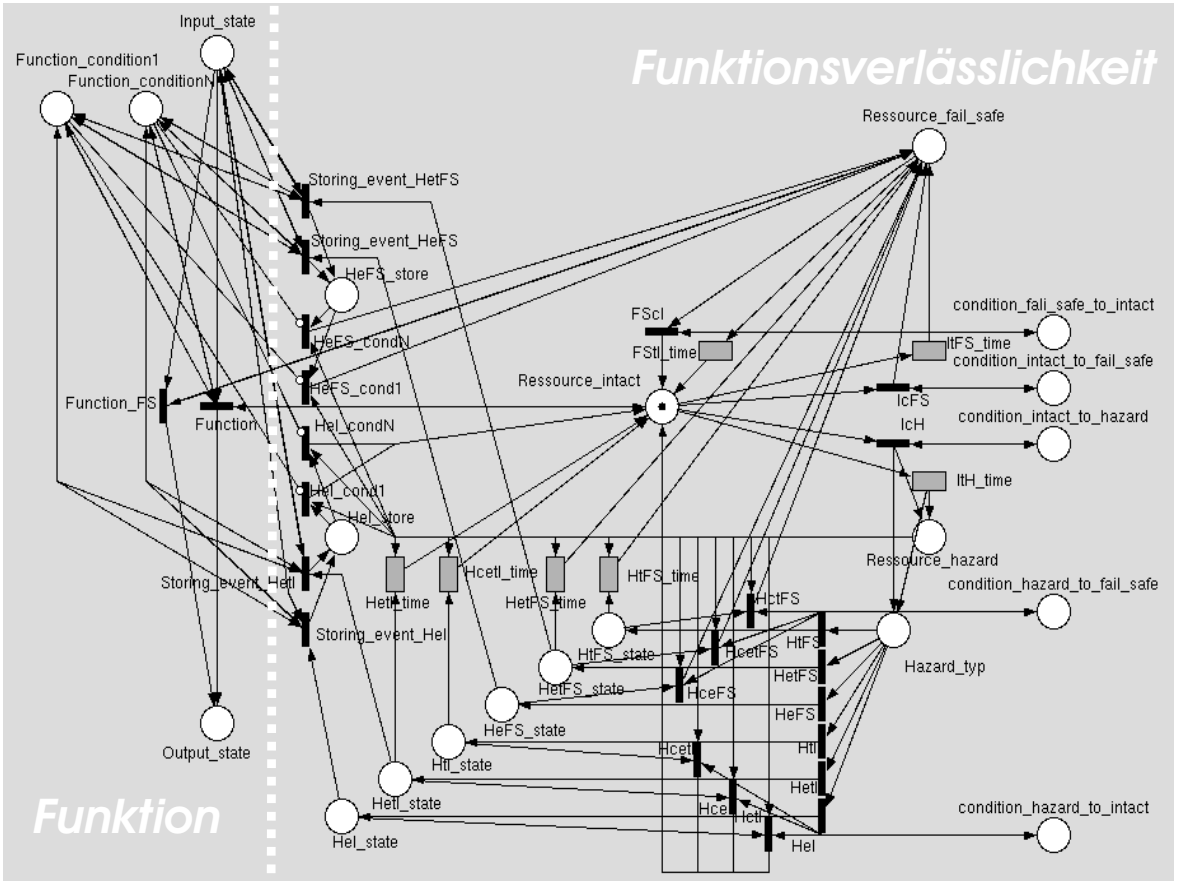

Abbildung 5.21: Generelle Verfeinerung des Verlässlichkeitsverhaltens einer hazard-passiven Funktion

ten von niedrigeren Sicherheitseigenschaften erfüllen zu können (s. weiter im Kapitel Systembeschreibung und Analyse).

Ortsbezogene Verlässlichkeitszustände Unter Anwendung der beschriebenen Methode kann jede Ressource in Bezug auf die durchgeführte Funktion um ihr Verlässlichkeitsverhalten erweitert werden. Im Falle einer hohen Abstraktionsebene, bei welcher eine Ressource für mehrere auch örtlich stark verteilte Funktionen verantwortlich ist, ist es oft notwendig, zusätzliche *ortsbezogene* Verlässlichkeitszustände in Betracht zu ziehen.
Ein ortsbezogener Ausfallzustand hat dann nur Auswirkungen auf diejenigen Unterfunktionen, für die die Ressource zuständig ist. Ein solcher Ausfall kann auch im Sinne der generellen Verlässlichkeitsmodellierung beschrieben werden, wobei er einen ereignis- oder zeitbezogenen Verlauf haben kann (s. Abb. 5.17 und 5.18).

Verlässlichkeit kurzgenutzter funktionaler Ressourcen Bei der funktionalen Verlässlichkeitsmodellierung müssen oft Verlässlichkeitszustände von Ressourcen betrachtet werden, deren Wirkungsdauer in dem modellierten Verhalten relativ zu deren temporalem Verlässlichkeitsverhalten sehr kurz ist. Eine vollständige Modellierung dieses Verhaltens würde den Modellumfang stark erhöhen, insbesondere im Falle einer höheren Anzahl solcher *kurzgenutzter* Ressourcen. Außerdem kommt es vor, dass eine Gesamtanzahl der beteiligten kurzgenutzten Ressourcen nicht bekannt ist, da diese von bestimmten temporalen Parametern der Modellierung abhängt (z.B. Anzahl der beteiligten Lokführer in einem modellierten Eisenbahnbetriebsprozess). Die kurzgenutzten funktionalen Ressourcen können dabei für eine Funktion auf Anforderung oder im Dauerbetrieb zuständig sein.
Da die Möglichkeit des Verlässlichkeitszustandswechsels der kurzgenutzten Ressource während ihrer Wirkungsdauer meistens sehr gering ist, kann die Dynamik des Verlässlichkeitsverhaltens vernachlässigt und durch eine statische Zustandsstruktur ersetzt werden. Die Modellierung beinhaltet dann anstatt der einzelnen stochastischen Übergänge zwischen den Verlässlichkeitszustände einer funktionalen Ressource nur probabilistisch gewichtete kausale Transitionen, die zum Zeitpunkt des Anfangs der Ressourceninanspruchnahme einmal über dem aktell für die Nutzung betrachteten Verlässlichkeitszustand der funktionalen Ressource entscheiden. Dieser gilt als konstant bis zum Ende der Beanspruchung der Ressource. Die probabilistischen Gewichte können vor ab, anhand der separaten Auswertung der stationären Auftrittswahrschweinlichkeiten einzelner Verlässlichkeitszustände des vollständiges Verlässlichkeitsmodells (Abb.5.19) der kurzgenutzten Ressource, ermittelt werden.
Abbildung 5.22 zeigt eine generelle Modellierung der Verlässlichkeit kurzgenutzter funktionaler Ressourcen. Die Wirkungsdauer dieser Ressource ist auf die Zeit zwischen der

Erfüllung der Anfangs- und der Endbedingung aus dem Modell des Eisenbahnbetriebes oder der Systemfunktionalität (*Begin-usage-condition* und *End-usage-condition*) beschränkt. Die Auswahl des aktuellen Verlässlichkeitszustandes erfolgt dann über die mit Auftrittswahrscheinlichkeiten (*W-intact*, *W-hazard* und *W-fail-safe*) gewichteten kausalen Transitionen. Die Inhibitoren zu den einzelnen Verlässlichkeitszuständen gewährleisten die Exklusivität ihren Auftretens.

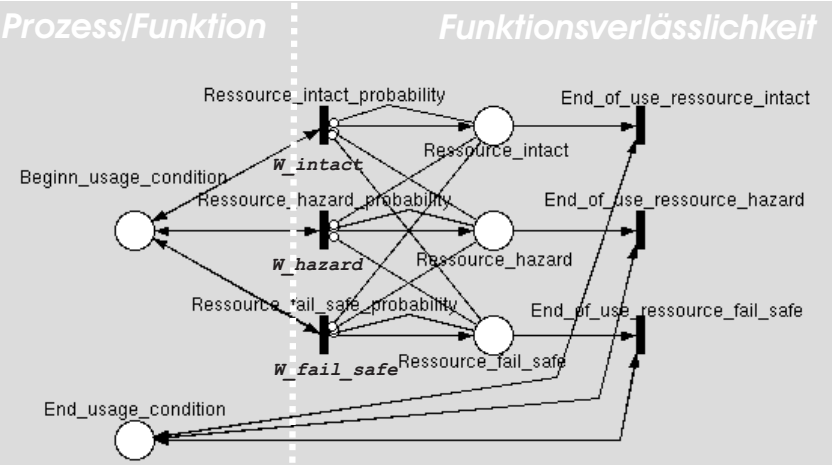

Abbildung 5.22: Generelle Modellierung des Verlässlichkeitsverhaltens einer kurzgenutzten funktionalen Ressource

Typische Beispiele der kurzgenutzten funktionalen Ressourcen bilden Ressourcen der Fahrzeugfunktionalität bei der *PROFUND*-Modellierung der streckenseitigen Systemfunktionsverlässlichkeit oder umgekehrt die streckenseitige Funktionalität bei der Modellierung der Verlässlichkeit von fahrzeugseitigen Systemfunktionen.

Beispiele der Verlässlichkeitsmodellierung

Beispiel aus der Bahnhofssicherung. Abbildung 5.23 zeigt die Erweiterung des funktionalen Modells der Stellung einer Fahrstrasse (Abb. 5.16) um das potentielle Verhalten, das aus der Betrachtung der Verlässlichkeit der zuständigen funktionalen Ressource - Fahrstraßensteuerung (*TRC - Train-Route-Control*) - resultiert.
Das potentielle Verlässlichkeitsverhalten ist im unteren Teil des Modells dargestellt, seine funktionalen Auswirkungen sind auf der linken Seite der Grafik abgebildet (die Modellerweiterung ist auch durch senkrecht stehende Transitionen des Verlässlichkeitsverhaltens gekennzeichnet).

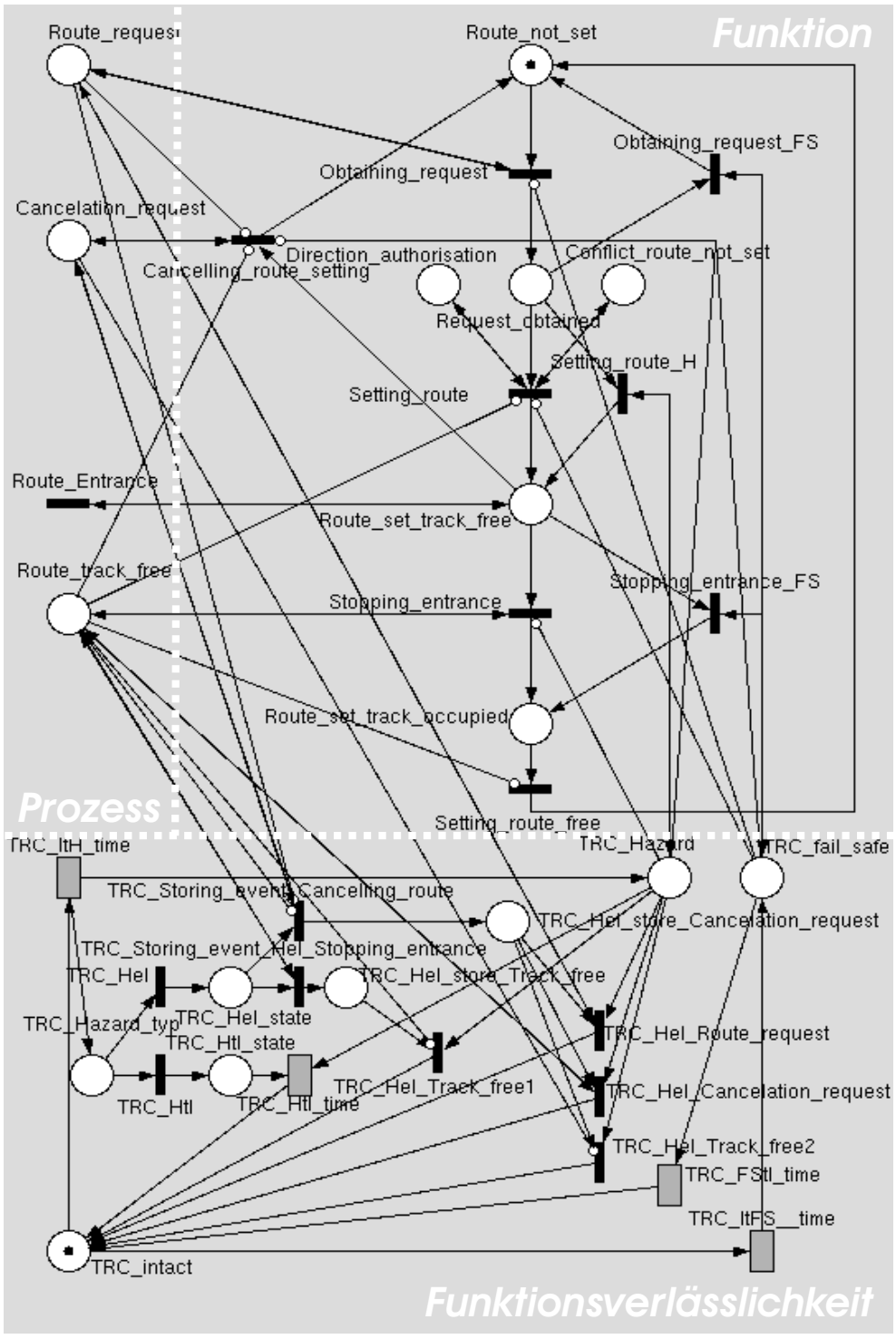

Abbildung 5.23: Modellierung des Verlässlichkeitsverhaltens der Funktion der Stellung einer Fahrstraße

Die graphische Darstellung der Abb.5.23 in Form eines EDSPN-Netzes ist z.T. unanschaulich. Eine übersictliche Darstellung ist mit Hilfe hierarchischer und farbiger Petrinetze (HCPN) möglich, dies wird weiter unten am Beispiel aus der Streckensicherung erläutert.
In der ursprünglichen Modellierung der Funktionsfolge zur Stellung einer Fahrstraße in Abb. 5.16 ist der Platz *Route-set-track-free* als Gefahrzustand für den Betrieb identifiziert, da dieser eine Einfahrt des Zuges in einen potentiell belegten bzw. nicht verschlossenen Fahrstraßenbereich (Gefahr einer Kollision bzw. Entgleisung) ermöglicht. Die Modellierung der Auswirkungen des Hazardzustandes der Ressource betrifft daher alle Teilfunktionen, die zu diesem Zustand führen (hazard-aktive Funktionen) bzw. die die Lage in diesem Zustand verlängern können (hazard- passive Funktionen). Konkret ist das hier die Teilfunktion *Setting-route* (führt zu dem potentiellen Hazardzustand) und die Teilfunktionen *Stopping-entrance* und *Cancelling-route-setting* (verlängern potentiell den Hazardzustand).
Im Rahmen der Modellierung des potentiellen Verhaltens wurden zwei Hazardverlaufsarten der Ressource betrachtet: Ein Hazardzustand, der eine bestimmte Zeitdauer vorliegt (modelliert durch die Transition *TRC-HtI-time*) und ein Hazardzustand, der bis zur Entdeckung nach erster Aufforderung durch den Betrieb andauert. Da diese zweite modellierte Hazardverlaufsart einerseits durch Rücknahme der Fahrstraßenstellung und andererseits durch Sperrung der Fahrstraßeneinfahrt beendet werden kann, müsste auch die Modellierung diese beiden Ereignisse und alle Auslösebedingungen berücksichtigen (kausale Transitionen *TRC-Storing-event-HeI-Cancelling-route* oder *TRC-Storing-event-HeI-Stopping-entrance* bzw. *TRC-HeI-Track-free1* oder *TRC-HeI-Route-request* oder *TRC-HeI-Cancellation-request* oder *TRC-HeI-Track-free2*).
In ähnlicher Weise wurde der Fail-Safe-Zustand der Fahrstraßensteuerung (*TRC-fail-safe*) modelliert (durch die Transition *TRC-ItFS-time*), wobei als sicherer Zustand der Zustand *Route-not-set* oder der Zustand *Route-set-track-occupied* angenommen wurde. Die Transitionen *Obtaining-request-FS* und *Stopping-entrance-FS* setzen den Fail-Safe-Zustand in der Funktionalität um. Der Fail-safe-Zustand wird nach dem Ablauf der durch die Transition *TRC-FStI* modellierten Zeit verlassen.

Beispiel aus der Streckensicherung. Die gleiche Methode der Modellbildung jedoch unter Ausnutzung der Hierarchisierung wurde bei der Erweiterung der prozessfunktionalen Modellierung des Streckenbeispieles (aus der Abb. 5.14) angewendet. Das erweiterte Modell der Funktionalität der Fahrwegsicherung mit seinen Submodellen zeigt Abbildung 5.24, wobei ein möglicher Gesamtausfall (Instanz *TRC123-dependability*) und drei ortsbezogene Ausfälle (identische Instanzen *TRC1-dependability* bis *TRC3-dependability*) der funktionalen Ressource (*TRC)* betrachtet wurden. Der Wirkungsbereich einzelner Ausfälle ist durch die Abfragekanten zu den zugehörigen Intaktzustän-

den definiert. Durch ihre logische AND-Verbindung ergibt sich die Markierung des globalen Intaktzustandes der Fahrwegsicherung (*TRC-intact*). Die einzelnen betrachteten Hazardzustände werden durch die aus den entsprechenden Verlässlichkeitsubmodellen stammende farbige Markierung des Platzes *TRC-hazard* modelliert.
Im Falle der betrachteten Funktionalität der Fahrwegsicherung wurde das Versagen der Funktion der Zugerkennung (*Det-train-block*) als Gefahr für den Betrieb angenommen. Der Fail-Safe-Zustand ist wiederum durch Erzwingen des Block-Besetzungszustandes (*Block-occ*) gegeben. Da ein Hazardzustand der Zugerkennung im Falle des Ausbleibens der Aktivierung dieser Funktion auftritt, wurde als Vorbild der Modellierung der Verlässlichkeitsubmodelle die generelle Verfeinerung des Verlässlichkeitsverhaltens einer hazard-passiven Funktion (Abb. 5.21) angewendet.
Jeder modellierte aufforderungsbegrenzte Hazardzustand (entsprechende farbige Marke auf dem Platz *TRC-hazard* und Abwesenheit der Marke auf dem entsprechenden Platz *TRC-intact1* bis *TRC-intact3*) wird durch ein Ereignis in dem Betriebsprozess erkannt. Dieses ist im Falle der modellierten ortsbezogenen Hazards eine gefährliche Situation (Anwesenheit von zwei Zügen in einem Block), die eine nicht korrekte Funktionsweise der Streckenblockfunktionalität offenbart. Nach der Hazardzustandsoffenbarung (Erlöschen des Zustandes des Beinaheunfalles - *Near-miss*) wird ein fail-safe Zustand des jeweiligen Streckenblocks eingenommen. Dieser wird erst nach der Reparatur wieder in den Intaktzustand überführt. Bei dem modellierten Gesamtausfall des Streckenblocks wird der Hazardzustand erkannt und in einen sicheren Zustand überführt, aber erst nach Ablauf der entsprechenden Zeitdauer der Transition (*TRC123-HtFS-time*). Diese Zeit repräsentiert die maximale Zeit der externen (nicht systemeigenen) Erkennung des gefährlichen Zustandes (im Sinne des Worst-Case). Als Grundlage zu ihrer Bestimmung können Daten aus dem Verkehrsprozess oder der allgemeinen Streckenüberprüfung oder Instandhaltung herangezogen werden.
Neben dem Verlässlichkeitsverhalten der streckenseitigen Sicherung muss auch die zugseitige Ausfallmöglichkeit der sicherheitsrelevanten Funktionalität modelliert werden. Abbildung 5.25 zeigt die entsprechende Modellierung als Verfeinerung der Instanz *Function-Train-Protection* aus Abbildung 5.14.
Betrachtet wird der Hazardausfall der Geschwindichkeitsüberwachung der Züge (zugentsprechende farbige Marken auf dem Platz *Trains-with-failed-ATP*), der zusammen mit einem nicht korrekten Verhalten des Lokführers (Missachten der Streckenblocksignale - modelliert durch zugentsprechende farbige Marken auf den Plätzen *Driver-SPAD-Sig1* bis *Driver-SPAD-Sig3*) zu einer unerlaubten Einfahrt in einen besetzten Streckenblock führen kann (Aktivierung entsprechender Transition *Tain-ignoring-Sig1* bis *Train-ignoring-Sig3* im Eisenbahnbetriebsprozess - in Mitte der oberen Abbildung). Die Geschwindigkeitsüberwachung (ATP -Automatic Train Protection) sowie das Verhalten des Lokführers wurden als eine kurzgenutzte funktionale Ressource modelliert,

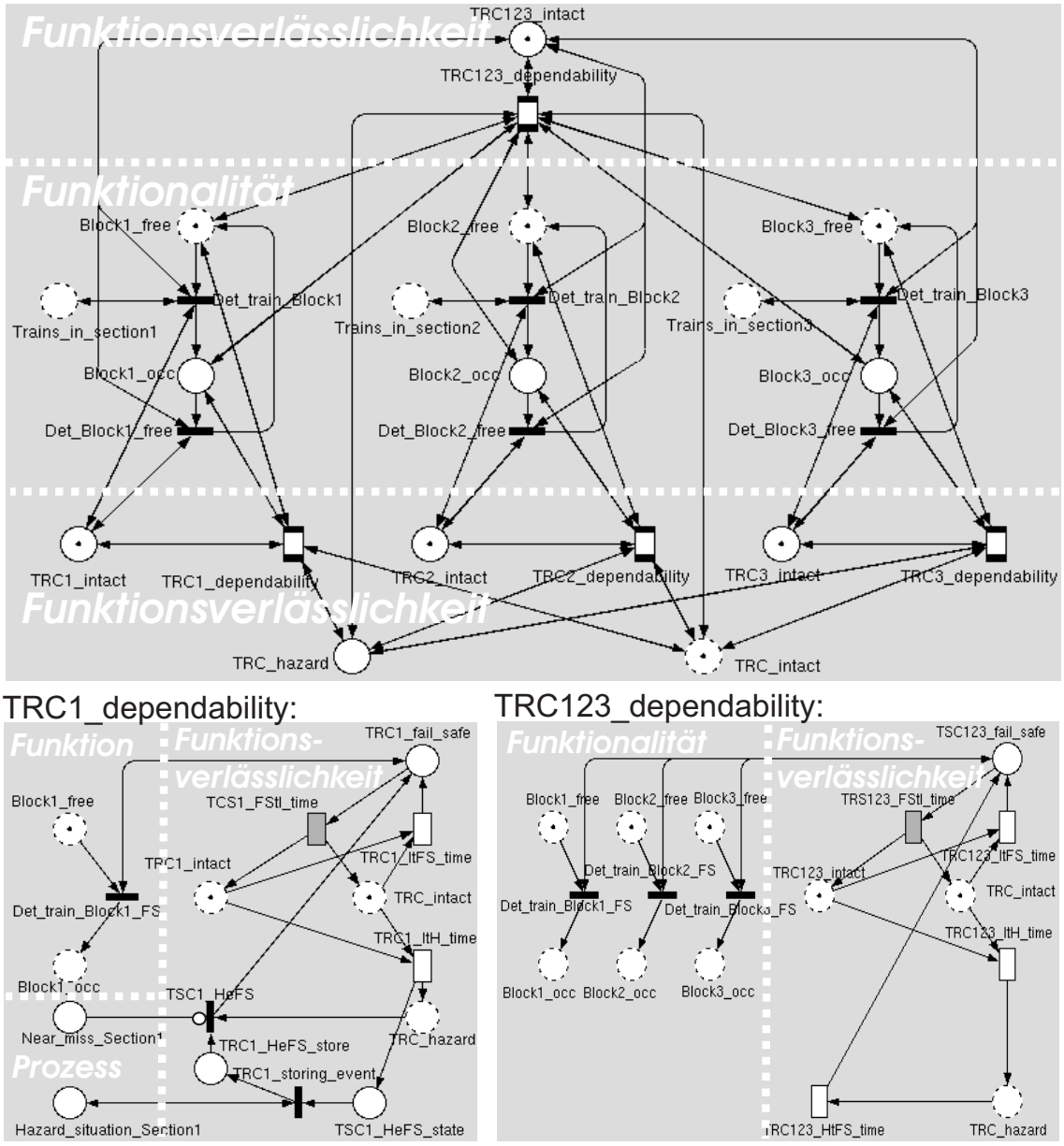

Abbildung 5.24: Erweiterung der Funktionalität der Fahrwegsicherung um Funktionsverlässlichkeit und zugehörige Verlässlichkeitsubmodelle

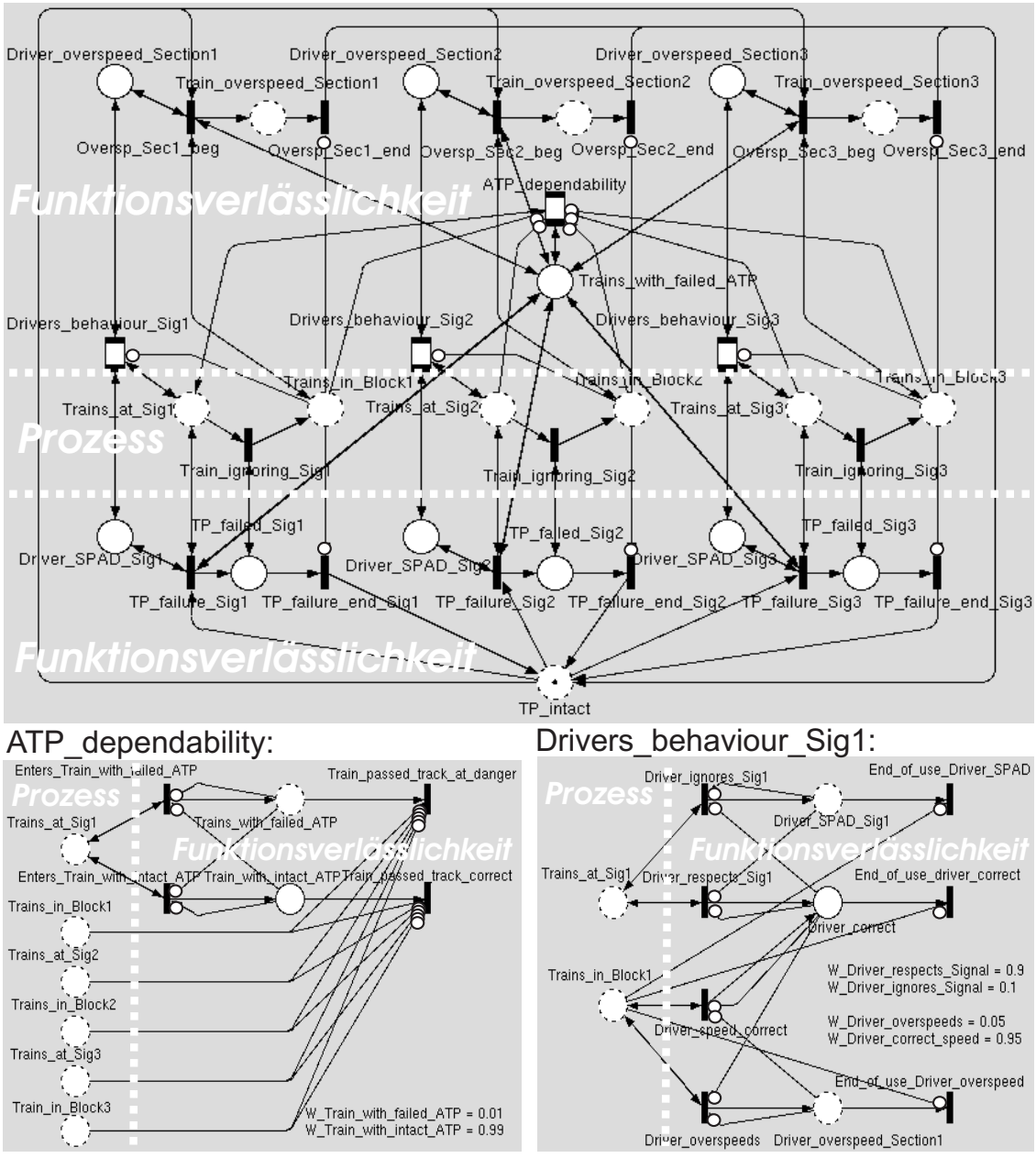

Abbildung 5.25: Funktionsverlässlichkeit der Fahrzeugsicherung und zugehörige Verlässlichkeitsubmodelle

deren Verlässlichkeitszustand sich während der Inanspruchsnahme nicht ändert. Im Falle der ATP ist ein konstanter Verlässlichkeitszustand während der gesamten Fahrt des Zuges durch die modellierte Strecke angenommen, die der Tatsache entspricht, dass die mittlere Hazardzustandsoffenbarungzeit von längerer Dauer als die längste Durchfahrtzeit eines Zuges ist. Im Falle des Lokführers wurde das Verhalten nur bei Vorbeifahrt an einem Signal als konstant angenommen, d.h. ein Verhaltenswechsel bis zum nächsten Signal ist möglich.
Die entsprechenden Submodelle mit Verlässlichkeit des ATP und des Verhaltens des Lokführers am ersten Signal (*ATP-dependability* und *Drivers-behaviour-Sig1*) sind im unterem Teil der Abbildung 5.25 dargestellt. Als Vorbild wurde die generelle Modellierung des Verlässlichkeitsverhaltens der kurzgenutzten funktionalen Ressource (Abb.5.22) herangezogen. Die Auftrittswahrscheinlichkeiten der betrachteten Verlässlichkeitszustände sind als probabilistische Gewichte der entsprechenden kausalen Transitionen in den Grafiken angegeben. Zur Vereinfachung wurde bei der ATP auch ihr streckenseitiger Teil (entsprechend der punkt- oder linienförmigen Zugbeeinflussung) in einem Verlässlichkeitsmodell zusammengefasst.
Neben der Betrachtung einer möglichen Missachtung der Streckensignale durch den Lokführer wurde auch eine unzulässige Beschleunigung während der Fahrt in einem Streckenabschnitt modelliert (Plätze *Driver-overspeed-in-Section1* bis *Driver-overspeed-in-Section3* in dem Submodell unten links auf der Abb. 5.25). Mit einem gleichzeitigen Ausfall der Geschwindigkeitsüberwachung (ATP) kann dieses Fehlverhalten zu einer Entgleisung (s. Modell der gefährlichen Situationen in Abb. 5.6) führen. Der probabilistische Gewichtfaktor (für jeden Streckenabschnitt spezifisch modelliert) gibt die Wahrscheinlichkeit des Auftritts dieser Unfallsituation an. Die zugentsprechende Farbe der Marke ermöglicht dann eine zugspezifische Auswertung des Risikos in dem Modell der Unfallereignisse in Abb. 5.5.

5.5 Beschreibung der Systemfunktionsimplementierung

Ziel der Beschreibung des Eisenbahnsicherungssystems ist die Darstellung der Abhängigkeit der Verlässlichkeit der Systemfunktionalität von der konkreten Art der Systemfunktionsimplementierung. In der Praxis bedeutet dies eine Erfüllung des Lastenheftes (funktionale Anforderungsspezifikation) durch ein Pflichtenheft (Entwurfspezifikation) des Systems. Die gleiche Aufgabe kann aus der Verlässlichkeitssicht gesehen werden, wobei die Verlässlichkeitsanforderungen des Lastenheftes durch Verlässlichkeitseigenschaften des Pflichtenheftes zu erfüllen sind.
Vor der Beschreibung des Eisenbahnsicherungssystems durch eine Modellierung ist ei-

ne vorläufige Gefahrenanalyse der beabsichtigten Systemimplementierung notwendig. Das Ergebnis dieser Gefahrenanalyse identifiziert die technischen Komponenten hinsichtlich ihrer Zuverlässigkeit, die die Verlässlichkeit des Eisenbahnbetriebes negativ beeinflussen kann. Hier sind die konventionellen top-down bzw. bottom-up Analysemethoden anzuwenden. Das gewählte Niveau der Abstraktion bildet die Basis für die darauf folgende Modellierung.
Im ersten Schritt der Beschreibung des Eisenbahnsystems ist die Systemimplementierung durch die Systemkomponenten zu konkretisieren und im zweitem Schritt sind die Abhängigkeiten unter den einzelnen Verlässlichkeitszuständen der Systemkomponenten zu beschreiben.

5.5.1 Modellbildung - Systemimplementierung

Die Implementierung der Systemfunktionen bedeutet die technische Realisierung der im Lastenheft spezifizierten funktionalen Ressourcen. Nach der funktionalen Modellierung ist jetzt eine Zuordnung der jeweiligen technischen Komponenten zu den einzelnen funktionalen Ressourcen erforderlich. Die Zuordnungsrelation ist wichtig, da im Prinzip jede funktionale Ressource durch eine oder mehrere Komponenten realisiert werden kann, andererseits kann auch eine Komponente eine oder mehrere Funktionen ausführen.
Abbildung 5.26 zeigt die Erweiterung der Funktions-Ressource Modellierung (Abb. 5.12) um die Zuordnungsrelation der Komponenten zu einer Ressource. Die Instanz (*Decomposition-instance*) repräsentiert die internen Verbindungen der Komponenten, die zu einer korrekten Funktionsfähigkeit der Ressource notwendig ist.

Beispiel aus der Streckensicherung. In Abbildung 5.27 ist eine mögliche Zuordnungsrelation der Komponenten der funktionalen Ressource "Zugfolgesicherung" (*Train-Sequence-Control*) aus Abbildung 5.14 dargestellt. Die Verfeinerungsinstanz (*Decomposition -Instance*) stellt die interne Verknüpfung der betrachteten Komponenten (Gleisstromkreise (*Track-Circuit*), Signale (*Signal*) und Auswertungslogik (*Computing-Logic*) dar.

Beispiel aus der Bahnhofssicherung. Abbildung 5.28 zeigt die funktionale Modellierung der Stellung einer Zugfahrstraße (aus Abb.5.16) und die mögliche Zuordnungsrelation zu den Komponenten der Implementierung der funktionalen Ressource der Fahrstraßensteuerung. Die ursprünglich durch einen Einzelplatz repräsentierte funktionale Ressource (*Train-Route-Control*) wurde der Unterfunktionen entsprechend zerlegt (Plätze *TRC1* bis *TRC5*) Die zugehörigen Instanzen (*DC1* bis *DC5*) bilden die Zuordnung zu den jeweiligen Implementierungskomponenten ab. Neben den

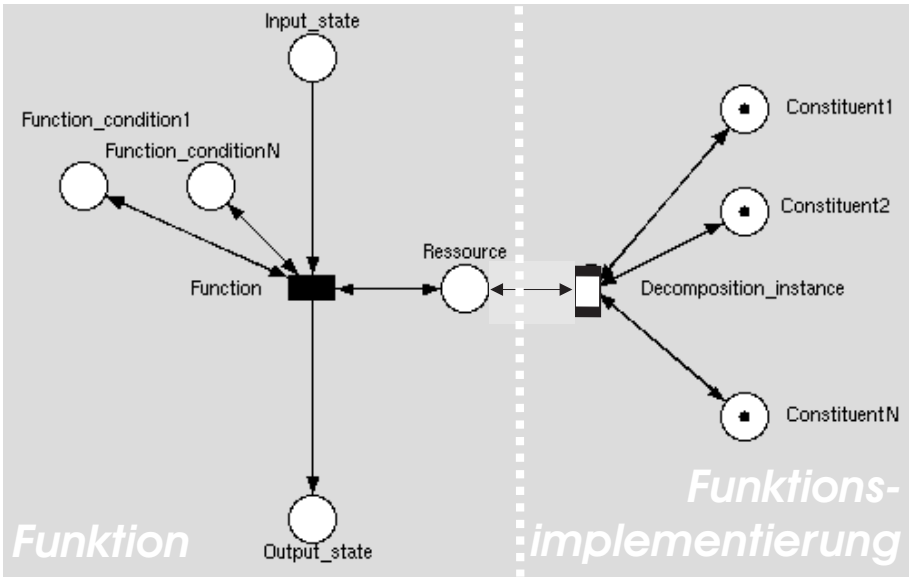

Abbildung 5.26: Implementierungskomponenten und deren Zuordnungsrelation zu der funktionalen Ressource

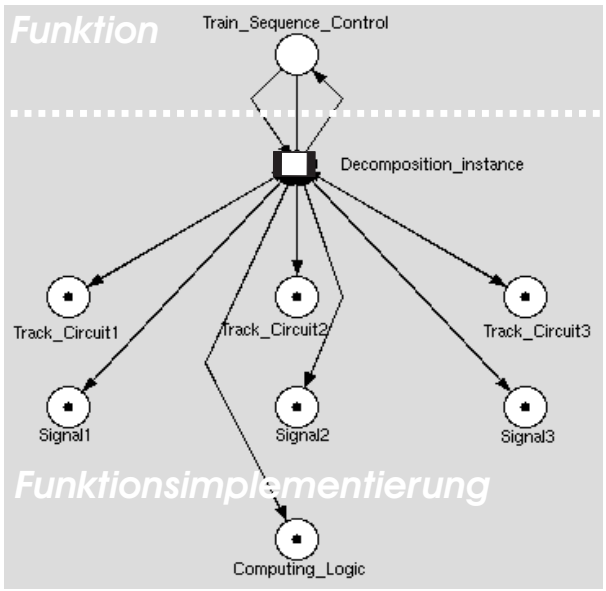

Abbildung 5.27: Implementierungskomponenten der Zugfolgesicherung

technischen Einrichtungen wie Gleisstromkreis des Annäherungs- und des Einfahrtsbereichs (*TC-station-approaching-area* und *TC-route-entrance-area*), Stellwerk (*Interlocking*) und Einfahrtsignal (*Sig-entrance*), wird hier auch die menschliche funktionale Verantwortung integriert. Die dargestellte Modellierung betrachtet die Beteiligung des Fahrdienstleiters (*Station-operator*) beim Empfang der Aufforderung zur Stellung der Fahrstraße sowie bei deren Rücknahme (Hilfsauflösung).

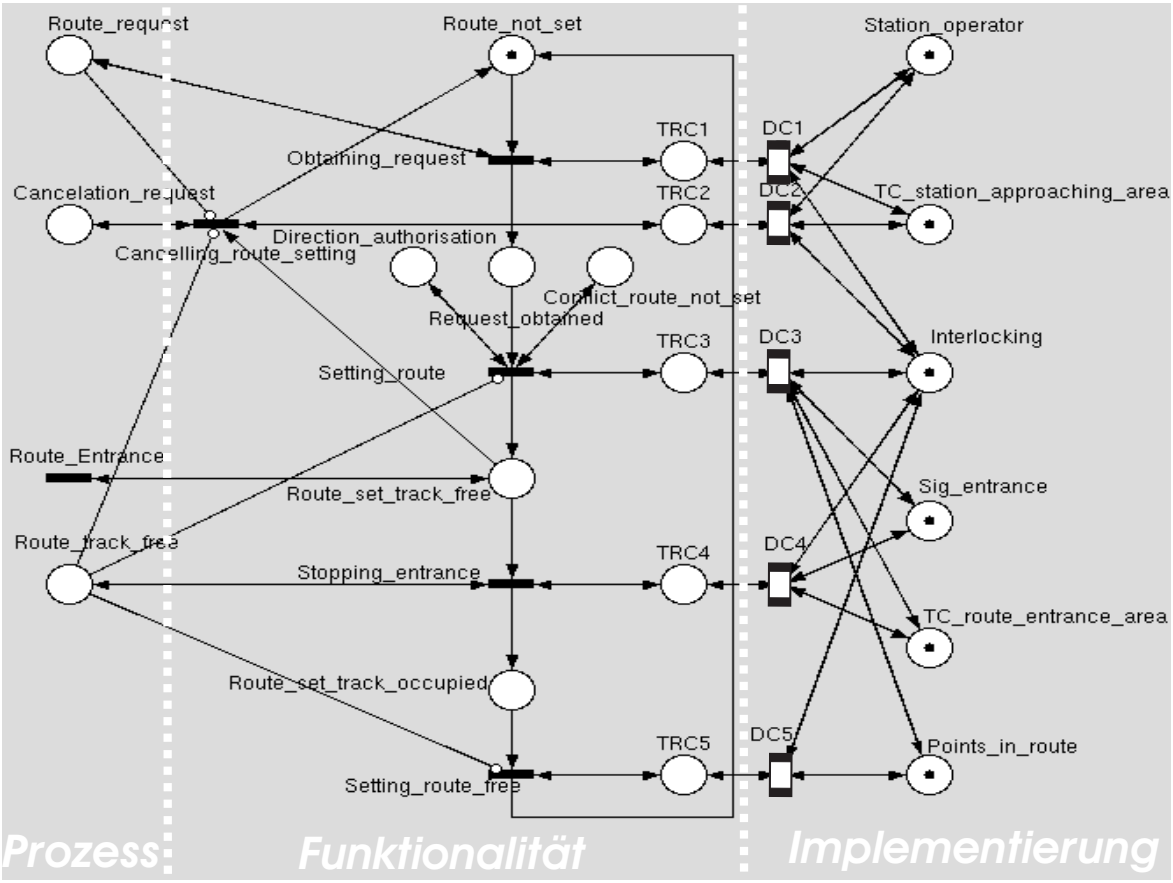

Abbildung 5.28: Implementierungskomponenten der Unterfunktionen zur Stellung einer Zugfahrstraße

5.5.2 Modellbildung - Systemimplementierungsverlässlichkeit

Die Aufgabe der Modellierung der Systemimplementierungsverlässlichkeit ist es, die Beziehungen zwischen den lokalen Verlässlichkeitszuständen der einzelnen Systemkomponenten (Betriebs- und Ausfallzustand) und den globalen Verlässlichkeitszuständen der zu implementierenden funktionalen Ressource (Intakt-, Fail-safe- und Hazardzu-

stand) zu beschreiben. Im Falle der komplexen Systemkomponenten, z.B. elektronische Komponenten, ist auch auf der Systemkomponentenebene zwischen sicheren und gefährlichen Ausfallzuständen zu unterscheiden.
Abbildung 5.29 zeigt eine prinzipielle Verbindung zwischen den Verlässlichkeitszuständen der funktionale Ressource und der Komponente, die in diesem Falle die gesamte Funktionalität implementiert. Die allgemeinen stochastischen Transitionen des gefährlichen und des fail-safe Ausfalles der zu implementierenden funktionalen Ressource (*ItH-time* und *ItFS-time*) sowie die Transition ihrer angenommenen Reparatur (*FStI-time*) des generellen Verlässlichkeitsmodells (Abb. 5.19) wurden hier durch zeitlose Transitionen ersetzt. Dagegen wurden die Transitionen der angenommenen externen Hazarderkennung aus der funktionalen Modellierung beibehalten und mit zusätzlichen parallelen zeitlosen Transitionen (*HtI-time* und *HtFS-time*) ergänzt. Die zeitlosen Transitionen repräsentieren daher die Wechsel der Verlässlichkeitszustände, die von der internen Systemimplemetierung abhängen. Die entsprechenden Testkanten sorgen dafür, dass ihr Schalten mit dem Verlässlichkeitszustandswechsel der Komponente synchronisiert ist.

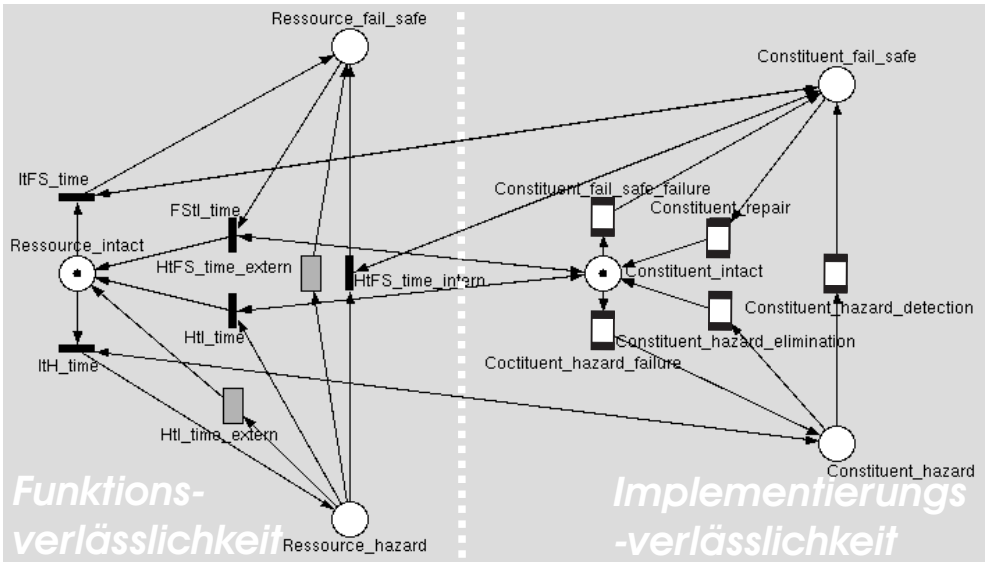

Abbildung 5.29: Verbindung zwischen der Funktions- und Implementierungsverlässlichkeit

Die höhere Anzahl der zu implementierenden Komponenten führt zu der Vermehrfachung der verbindenden Testkanten bzw. zeitlosen Transitionen. Die Verbindung zwischen den lokalen und den globalen Verlässlichkeitszuständen auf der Komponenten- und Funktionsebene kann die gegenseitigen internen stochastischen Abhängigkeiten im Verlässlichkeitsverhalten zwischen den Komponenten abbilden. Ein Beispiel, in dem

eine funktionale Ressource durch zwei stochastisch unabhängige Komponenten implementiert wurde, zeigt die im Weiteren erklärte Abbildung 5.30.

Beispiel aus der Streckensicherung. Abbildung 5.30 zeigt eine Verfeinerung der technischen Implementierung der funktionalen Ressourcen der Fahrwegsicherung aus Abbildung 5.27. Die hier modellierte Implementierung setzt einen Gleisstromkreis zum Zweck der Zugdetektion und Gleisfreimeldung und ein Signal als Kommunikationsmittel zur Information des Lokführers voraus. Das dargestellte Modell entspricht der Verfeinerung der Instanz *TRC1-dependability* aus der Abb.5.24.

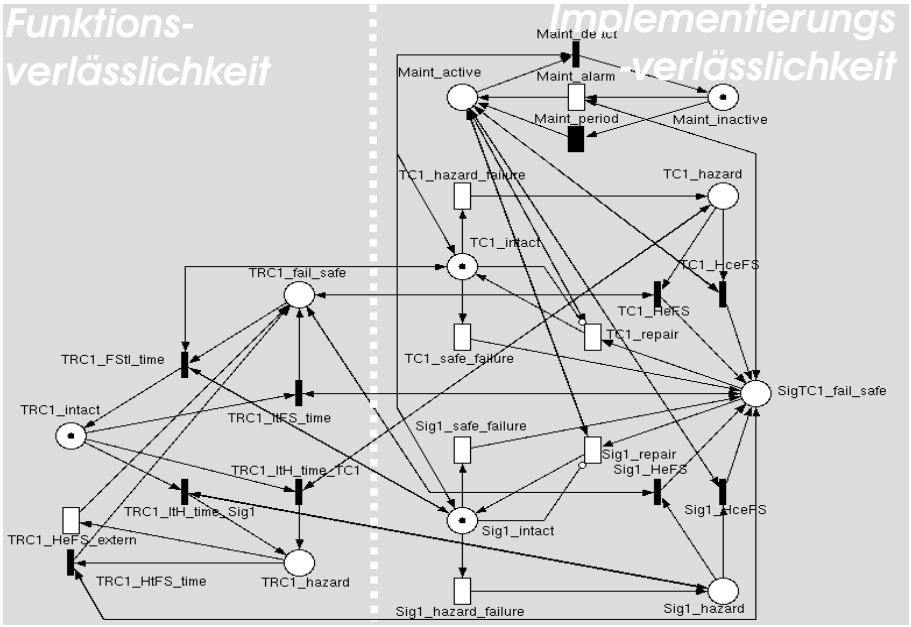

Abbildung 5.30: Verlässlichkeitsverhalten des Gleisstromkreises und des Signals als Implementierungskomponenten der Fahrwegsicherung

Die Modellierung betrachtet bei jeder dieser Komponenten die Möglichkeiten eines sicheren und eines gefährlichen Ausfalles, sowie deren Offenbarung und Reparatur, wobei die Bezeichnung der Transitionen der in dem Kapitel Funktionsverlässlichkeit (Kap.5.4.2) definierten entspricht.
Die Plätze *TC1-hazard* und *Sig1-hazard* repräsentieren die genannten gefährlichen Ausfallzustände der Komponenten. Die Offenbarung dieser Verlässlichkeitszustände kann entweder durch Eingriff einer periodischen Instandhaltung (Belegung des Platzes *Maint-active* durch Schalten der Transition *Maint-period*) oder durch eine externe Erkennung aus dem Eisenbahnbetriebsprozess erfolgen, die hier durch eine exponentialverteilte Ersatztransition *TRC1-HeFS-extern* modelliert ist. Nach einer solchen

externen Hazardzustandserkenung sowie im Falle eines sicheren Ausfalles modellierter Implementierungskomponenten (*TC1-ItFS* und *Sig1-ItFS*) wird die Instandhaltung innerhalb der durch die Transition *Maint-alarm* modellierten Dauer aktiviert. Die Aktivierung der Instandhaltung bildet eine Voraussetzung zur Durchführung der Reparatur einzelner oder beider ausgefallenen Komponenten (Schalten der Transition *TC1-FStI* bzw. *Sig1-FStI*). Im Modell spiegelt sich die Annahme wider, dass ein sicherer Ausfallzustand oder ein erkannter Hazardzustand einer Komponente die Erkennung des Hazardzustandes auch der anderen Komponenten (modelliert durch kausale Transitionen *TC1-HceFS* bzw. *Sig1-HceFS*) bedingt.

Beispiel einer 3-kanaligen Implementierungskomponente Abbildung 5.31 zeigt das Implementierungsmodell der Auswertungslogik als einer weiteren Komponente der funktionalen Ressource "Fahrwegsicherung" (s. Abb.5.27) - durch eine dreikanalige Architektur (z.B. Rechnerkanäle). Es handelt sich um eine Steuerungskomponente, deren Verlässlichkeitszustand alle weiteren Komponenten der Fahrwegsicherung beeinflusst. Das funktionale Verlässlichkeitsmodell ist in Abb. 5.24 dargestellt (*TRC123-dependability*).

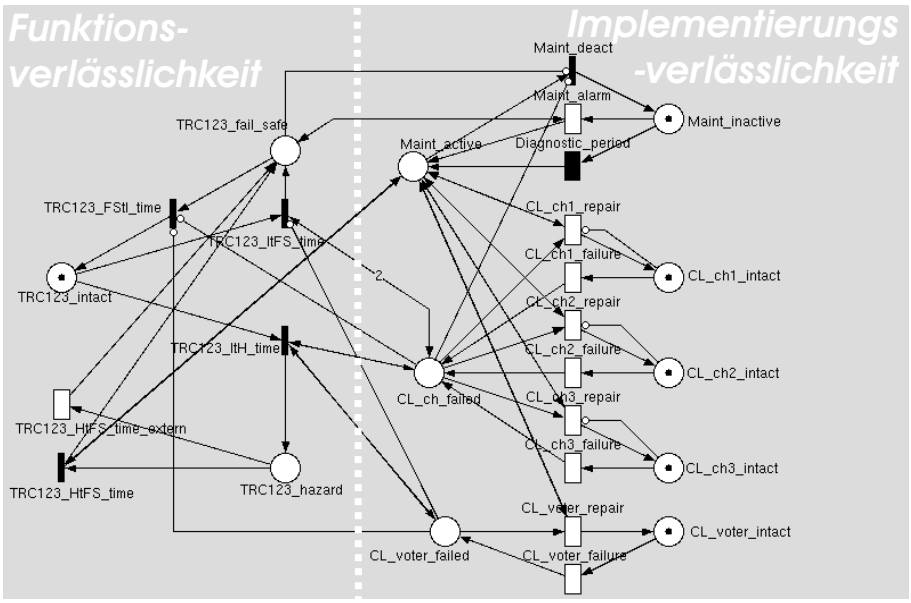

Abbildung 5.31: Verlässlichkeitsverhalten der Auswertungslogik als Implementierungskomponenten der Fahrwegsicherung

Die Ausgänge der Kanäle werden durch einen Voter verglichen. Die einzelnen Kanäle sowie der Voter können ausfallen (modelliert durch die entsprechenden *failure*-Transitionen).

Die Anzahl der ausgefallenen Kanäle entspricht der Tokenanzahl auf dem Platz *CL-ch-failed*. Die Reparatur aller Komponenten ist nur durch einen aktiven Instandsetzungseingriff möglich (Belegung des Platzes *Maint-active*). Die Aktivierung der Instandhaltung erfolgt entweder periodisch in einem diagnostischen Zyklus (Transition *Diagnostic-period*) oder ereignisbedingt (Transition *Maint-alarm*) nach Erreichung eines fail-safe Zustandes.
Die modellierte Komponentenstruktur toleriert den Ausfall eines Rechnerkanals, wobei die Korrektheit des Verhaltens durch den Voter gewährleistet ist. Sein Ausfall in Verbindung mit dem Ausfall mindestens eines Rechnerkanals führt zu einem globalen Hazardzustand (Platz *TRC123-hazard*) auf der funktionalen Ebene der Ressource. Die zugehörige zeitlose Transition *TRC123-ItH-time* entspricht der allgemeinen stochastischen Transition des funktionalen Verlässlichkeitsmodells in Abb. 5.24. Die Erkennung des Hazardzustandes erfolgt entweder extern, durch die Transition *TRC123-HtI-time-extern* aus dem Funktionsverlässlichkeitsmodell, oder durch die periodische Diagnostik. Im Vergleich zum Verlässlichkeitsmodell *TRC1-dependability* wird bei der Rechnerlogik keine Erkennung des Hazardzustandes aus dem Eisenbahnbetriebsprozess betrachtet. Ebenso sind die Übergänge zum globalen Fail-safe-Zustand (*TRC123-fail-safe*) einerseits durch Ausfall von mindestens zwei Kanälen bei intaktem Voter (Transition *TRC123-ItFS-time*) und andererseits durch die Erkennung des Hazardzustandes im Rahmen des diagnostischen Zyklus (Transition *TRC123-HtFS-time*) modelliert. Nach Beseitigung der Ausfallzustände aller Komponenten wird der globale Intaktzustand (Platz *TRC123-intact*) durch Schalten der zeitlosen Transition *TRC123-FStI-time* erreicht.
Ein Beispiel der Verlässlichkeitsmodellierung einer zweikanaligen Architektur kann in einer früher dargestellten Abbildung 4.5 gefunden werden. Weitere Petrinetzmodelle der Implemetierungsverlässlichkeit finden sich z.B. in [Schneeweiss 1999].
Der Grad der Verfeinerung der globalen Verlässlichkeitsmodellierung der Implementierung entspricht dem Verfeinerungsgrad der Verlässlichkeitsmodellierung der funktionalen Ressource. In der praktischen Anwendung der Methode ist es oft notwendig, auch auf der funktionalen Ebene die Auswirkung der Hazardzustände einzelner Implementierungskomponenten zu betrachten, da eine rein globale Sicht, in der jeder Hazardzustand einer Komponente als ein Hazardzustand des Gesamtsystems gesehen wird, oft zur Überdimensionierung der Sicherheitsanforderungen führen kann.

5.6 Zusammenfassung

Die Aufgabe der *PROFUND*-Modellierung ist es, den Eisenbahnprozess, die Systemfunktionalität sowie die Funktions- und Systemimplementierungsverlässlichkeit so zu beschreiben, dass der Bezug zwischen dem betrieblichem Risiko und der Systemverläs-

slichkeit hergestellt werden kann. Die angewendete Methode erlaubt durch Verwendung des geeigneten Beschreibungsmittels eine strenge Modularität der einzelnen Betrachtungsgegenstände, d.h. der Teilmodelle. Ziel des dargestellten methodischen Vorgehens ist es, im ersten Schritt aus dem zulässigen betrieblichen Risiko die funktionalen Sicherheitsanforderungen in Form von zulässigen maximalen Hazardraten und minimalen Hazarderkennungs- und Beseitigungsraten abzuleiten (Risikoreduktion). Im zweiten Schritt sind unter Verwendung der Modellierung die Parameter der Implementierungsverlässlichkeit (Ausfall-, Detektion-, Reparaturraten) zu ermitteln, damit die funktionalen Sicherheitsanforderungen erfüllt werden.
Die Genauigkeit und der Detaillierungsgrad der Modellierung hängen stark von den zugänglichen statistischen Daten bzw. Verteilungen ab. Eine besondere Bedeutung haben auch die Schätzungen der Wahrscheinlichkeitsgewichte der einzelnen betrachteten Ausfallverlaufsarten. Bei Unzugänglichkeit der Daten muss in der Modellierung immer eine Worst-Case Schätzung vorgenommen werden.
Das detaillierte Vorgehen bei den quantitativen Modellauswertungen ist Gegenstand des nächsten Kapitels *PROFUND*-Analyse.

Kapitel 6

PROFUND-Analyse

6.1 Ziele der Modellanalyse

Das grundlegende Ziel einer Modellanalyse ist es, für ein explizit beschriebenes Modell das implizit beschriebene Modellverhalten zu untersuchen. Da jede Modellierung auf einer bestimmten Abstraktion der Realwelt basiert, kann die Modellanalyse dabei aus zwei unterschiedlichen Sichten durchgeführt werden. Einerseits ist es die Sicht der Modellverifikation, in der das Modell auf das korrekte Verhalten im Rahmen der gewählten Abstraktion geprüft wird, anderseits ist es die Modellvalidation, in der das erzielte Modellverhalten mit dem Verhalten der Realwelt verglichen wird. Die Verbindung zu traditionellen Techniken der Sicherheitsanalyse bildet ein Mittel zur Modellvalidation (vgl. Kap.2) und zur Einführung in die praktische Anwendung des vorgestellten Vorgehens. Nur ein valides Modell kann zur Definition der Sicherheitsanforderungen im Sinne des Vorgehens bei der Anwendung der *PROFUND*-Methode (Abb. 5.1) herangezogen werden.
Da im Vordergrund dieser Arbeit das Potential des formalen Beschreibungsmittels der Petrinetze steht, beziehen sich die vorgestellten Analysetechniken schwerpunktmäßig auf die Modellverifikation. Zur Vorstellung des methodischen Vorgehens werden daher Beispieldaten ohne direkten Bezug auf ein konkretes Realobjekt verwendet.

6.2 Risikoanalyse des Eisenbahnbetriebes

Das Modell des Eisenbahnbetriebes, dessen Bildung in Kapiteln 5.3 und 5.4 vorgestellt wurde, beschreibt den physikalischen Prozess des Eisenbahnverkehrs, die Funktionalität seiner Steuerung sowie deren Verlässlichkeit. Im Sinne der *PROFUND*-Methode (Abb.5.1) ist es möglich, das Modell des Eisenbahnbetriebes zusammen mit dem Modell der Unfallfolgen zur Auswertung des betrieblichen Risikos zu verwenden. Eine

Voraussetzung glaubwürdiger Ergebnisse ist eine erfolgreiche Modellverifikation und -validation. Das Vorgehen wird in den folgenden Unterkapiteln vorgestellt.

6.2.1 Analyse des Modells des Betriebsprozesses

Das Modell des Betriebsprozesses wurde unter Kenntnis der konkreten Betriebsverhältnisse einer konkreten Bahninfrastruktur und auf der Basis der Ergebnisse der Gefahrenanalyse aufgebaut. Dieses bildet die Bezugsgrundlage der Modellverifikation und -validation.

Modellverifikation

Neben der Prüfung des Bezuges zur gewählten Abstraktion der Realwelt beinhaltet die Aufgabe der Modellverifikation auch die Prüfung der korrekten Verwendung des Beschreibungsmittels (Syntax check). Bei der Anwendung der EDSPN's beinhaltet diese z.B. die Prüfung der korrekten Verknüpfung zwischen den Knoten (Plätzen und Transitionen) oder die Prüfung der eindeutigen Knotenbezeichnung und -parametrierung.
Eine Vorstufe der Modellverifikation ist die interaktive Simulation des Modellverhaltens. Durch Identifikation der Ereignisse (repräsentiert durch Transitionen) mit erfüllten Auftrittsbedingungen hat der Anwender die Möglichkeit, die grundlegenden Prozesse der gewählten Abstraktion des Eisenbahnprozesses interaktiv abzuspielen, indem er selbst das Modellverhalten durch Transitionsaktivierung steuert (Markenspiel). Da bei dieser Art der Simulation die Zeitparameter (deterministische oder stochastische) temporaler Ereignisse nicht berücksichtigt werden, ist es möglich, auch ganz seltene Ereignisfolgen auf die Korrektheit der Beschreibung zu prüfen.

Erreichbarkeitsgraph Der Nachteil der interaktionsbasierten Simulation ist die fehlende Garantie der Vollständigkeit. Diese kann nur durch ein automatisches Abspielen aller möglichen Ereignisfolgen des Modellverhaltens erzielt werden. Eine vollständige Darstellung aller Ereignisfolgen ist durch den Erreichbarkeitsgraph des Petrinetzes gegeben. Der Erreichbarkeitsgraph beschreibt auch den vollständigen Zustandsraum (RS - Reachability set, bzw. auch EG) $RS := [m_0 >$ des durch das Petrinetz beschriebenen Verhaltens, wobei m_0 die Initialmarkierung des Petrinetzes ist.
Jede erreichbare Markierung m aller Petrinetzplätze ist durch einen Knoten des Erreichbarkeitsgraphen vertreten. Eine konkrete Markierung eines einzigen Petrinetzplatzes ist aber durch eine Menge von Knoten aus RS repräsentiert.
Abbildung 6.1 zeigt den Erreichbarkeitsgraphen des Modells des Betriebsprozesses aus dem Unterkapitel 5.3.1 (dargestellt in Abbildungen 5.5, 5.6 und 5.7). Der Graph stellt lediglich die zeitbehafteten Zustände des Erreichbarkeitsgraphen dar (*tangible markings*), also die Zustände, die nur durch das Schalten einer temporalen Transition

verlassen werden können. Diese Zustände umfassen auch alle davor stehenden zeitlosen Zustände (*vanishing markings*), deren Auftritt von der Aktivierung einer kausalen Transition gefolgt ist (z.B. die probabilistisch gewichteten kausalen Transitionen *Near-miss-event-Section1* und *Accident-event-Section1* sind in der vorherigen temporalen Transition *Two-trains-in-Section1* enthalten, s. Abb. 5.6).

Graph von Mengen globaler Zustände Der Graph von Mengen globaler Zustände repräsentiert eine kondensierte Darstellung des Erreichbarkeitsgraphen, in dem Knoten mit einer bestimmten Eigenschaft zusammengefasst werden. Allgemein kann daher ein Knoten diesen Graphen κ als

$$\kappa := \{m \in RS | P_\kappa(m)\} \tag{6.1}$$

definiert werden, wobei κ für alle Markierungen m (Zuständen) steht, die die durch das Prädikat P_κ spezifizierte Eigenschaft besitzen.
Die rot markierten Knoten des Graphen in Abbildung 6.1 repräsentieren also alle Zustände des Modellverhaltens in denen das unerwünschte Ereignis *Kollision* aufgetreten ist. Gemeinsam bildet diese Menge der Knoten den globalen Unfallzustand *Accident*, dessen Auftrittshäufigkeit für die Risikoauswertung entscheidend ist. Der Globale *Unfallzustand* U ist definiert als:

$$U := \{m \in RS | P_U(m)\} = \{m \in RS | m(Accident) = 1\} \tag{6.2}$$

wobei $m(Accident) = 1$ für alle Zustände des Erreichbarkeitsgraphen mit markiertem Platz *Accident* steht.
Auf die gleiche Weise können die Knoten des Erreichbarkeitsgraphen identifiziert werden, die zu den gefährlichen Situationen in dem Betriebsprozess gehören (gelb markiert). In dem Beispiel aus der Streckensicherung sind es die Situationen, bei welchen sich zwei oder mehrere Züge in einem betrachteten Streckenabschnitt gleichzeitig befinden, ohne dass sie zu dem globalen Unfallzustand gehören. Daher kann der globale Zustand *gefährliche Situation GS* wie folgt definiert werden:

$$GS := \{m \in RS \setminus U | m(\textit{Trains-in-Section } S) = 2, S \in \{1, 2, 3\}\} \tag{6.3}$$

Alle anderen Knoten des Erreichbarkeitsgraphen, die weder zu dem globalen Zustand Unfall noch zu dem globalen Zustand gefährliche Situation gehören, stellen das *Regelverhalten RV* des modellierten Eisenbahnprozesses dar (grün markiert). Die Menge der Zustände des Regelverhaltens kann daher wie folgt definiert werden:

$$RV := RS \setminus (U \cup GS). \tag{6.4}$$

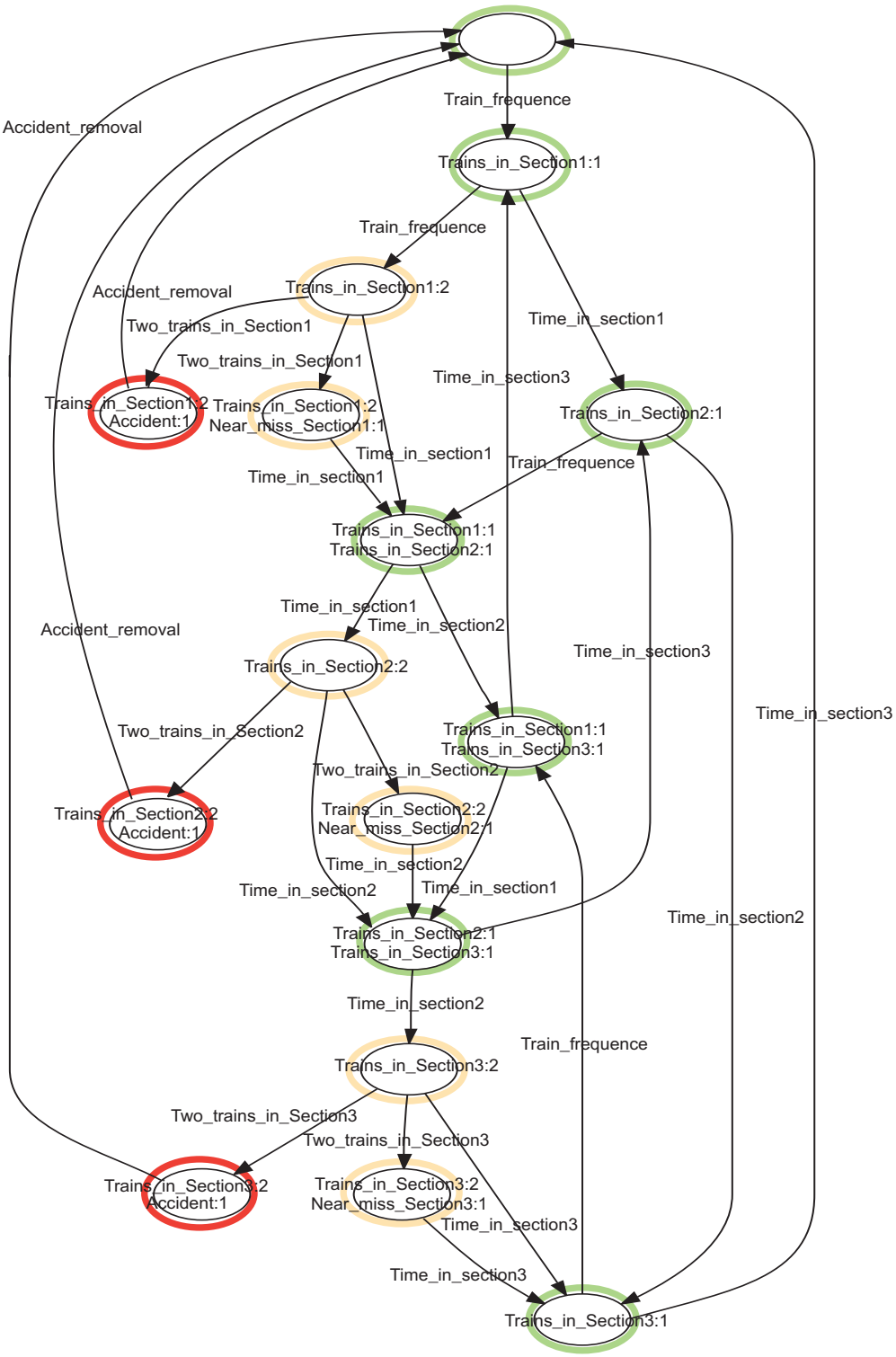

Abbildung 6.1: Erreichbarkeitsgraph des Modells des Betriebsprozesses

Tabelle 6.1 zeigt eine tabellarische Darstellung der Knoten des Erreichbarkeitsgraphen mit der Angabe der vollständigen Knotenmarkierung. Entsprechend der Belegung der relevanten Plätze gibt die farbige Kodierung die Zugehörigkeit des jeweiligen Knotens zu den definierten globalen Mengen an.

		Markierung des EG Zustandes						
EG Zustand		Trains_in_Section1	Trains_in_Section2	Trains_in_Section3	Near_miss_Section1	Near_miss_Section2	Near_miss_Section3	Accident
RV	0_t	0	0	0	0	0	0	0
RV	1_t	1	0	0	0	0	0	0
GS	2_t	2	0	0	0	0	0	0
RV	3_t	0	1	0	0	0	0	0
RV	4_t	1	1	0	0	0	0	0
GS	5_t	2	0	0	1	0	0	0
U	13_a	2	0	0	0	0	0	1
RV	6_t	0	0	1	0	0	0	0
GS	7_t	0	2	0	0	0	0	0
RV	8_t	1	0	1	0	0	0	0
RV	9_t	0	1	1	0	0	0	0
U	14_a	0	2	0	0	0	0	1
GS	10_t	0	2	0	0	1	0	0
GS	11_t	0	0	2	0	0	0	0
U	15_a	0	0	2	0	0	0	1
GS	12_t	0	0	2	0	0	1	0

Tabelle 6.1: Tabellarische Darstellung der Knoten des Erreichbarkeitsgraphen des modellierten Betriebsprozesses

Abbildung 6.2 abstrahiert die globalen Mengen *U*, *GS* und *RV*. Die Zahlen innerhalb der dargestellten Mengen geben nur die entsprechende Anzahl der zugehörigen Knoten (Zustände) an. Daneben repräsentieren die verbindenden Kanten die Transitionen, die zum Übergang zwischen zwei Mengen führen.

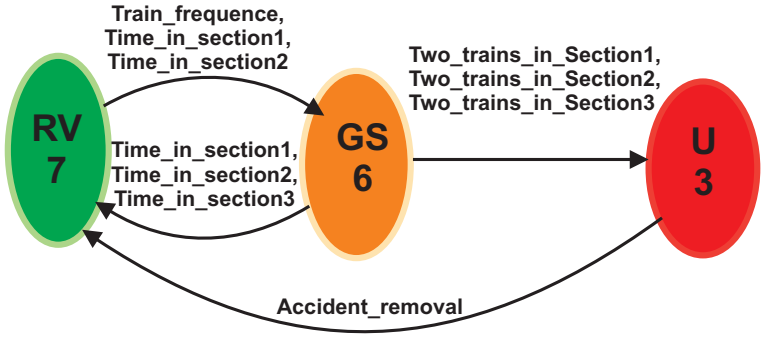

Abbildung 6.2: Graph von Mengen globaler sicherheitsrelevanter Zustände des Modells des Eisenbahnbetriebsprozesses

Eine solche Darstellung der sicherheitsrelevanten globalen Zustandsmengen gibt einen notwendigen Überblick über die Dynamik des analysierten Modells aus Sicht der Si-

cherheitsbetrachtung. Es zeigt die zeitlichen bzw. kausalen (je nach Typ der Übergangstransition) Folgen der Ereignisse die zu dem unerwünschten Ereignis des modellierten Systemverhaltens führen.

Unfallbaum Die zweite Grundlage der Beurteilung der Korrektheit der Modellierung bildet die statische Analyse des erreichten unerwünschten Zustandes im modellierten Verhalten des Eisenbahnprozesses. Basis dazu bildet die Markierung sicherheitsrelevanter Plätze in allen Knoten der Menge des globalen Unfallzustandes.
Im Rahmen der vorgestellten *PROFUND*-Methode sind die sicherheitsrelevanten Plätze einerseits durch die Plätze des Prozessmodells (*P-Plätze*) gebildet, die im direkten Bezug zu den unerwünschten risikobehafteten Ereignissen stehen, anderseits durch die Plätze des Verlässlichkeitsmodells (*V-Plätze*) die wiederum in direktem Bezug zu den Ursachen der Fehlzustände der Systemfunktionalität bzw. -implementierung stehen. Da sich die Markierung der Plätze der Systemfunktionalität, bzw. -implementierung *(F-, bzw. I-Plätze)* selbst auf das korrekte Modellverhalten bezieht, werden diese Plätze in die statische Analyse unerwünschter Prozesszustände nicht direkt einbezogen, kann jedoch als wichtige Quelle der Kontextinformationen herangezogen werden.
Sollte das Modell des Betriebsprozesses mehrere Abstraktionsebenen umfassen, sind die P-Plätze jeder weiteren Unterebene als *PP-Plätze*, (bzw. *PPP-Plätze*, usw.) zu bezeichnen.
Tabelle 6.2 zeigt die sicherheitsrelevanten Plätze der EG-Knoten der globalen Menge des Unfallzustandes des betrachteten Modells des Eisenbahnbetriebsprozesses. Diese sind in diesem Falle lediglich durch die P-Plätze gebildet. Als sicherheitsrelevant gilt dabei nur die Markierung mit mindestens zwei Marken, die die gleichzeitigen Besetzung des Streckenabschnittes mit zwei Zügen abbildet und die Voraussetzung für einen Unfall darstellt.

	Markierung des EG Zustandes			
	U	**P1**	**P2**	**P3**
EG Zustand	Accident	Trains_in_Section1	Trains_in_Section2	Trains_in_Section3
13_a	1	2	0	0
14_a	1	0	2	0
15_a	1	0	0	2

Tabelle 6.2: Plätze sicherheitsrelevanter Knoten des Erreichbarkeitsgraphen

Aus der Tabelle ist ersichtlich, dass der Unfall entweder im Abschnitt1 oder Abschnitt2 oder Abschnitt3 (Section) auftreten kann. Diese Beziehung kann auch durch folgende Gleichung ausgedrückt werden:

$$U = P1 + P2 + P3. \tag{6.5}$$

Abbildung 6.3 zeigt die entsprechende graphische Darstellung unter Benutzung der Semantik der Störungsbäume (*FTA*). Ein so entstandener Unfallbaum kann auf diese Weise unter Betrachtung weiterer sicherheitsrelevanter Plätze der globalen Menge des Unfallzustandes weiter entwickelt werden (s. weitere Kapitel).

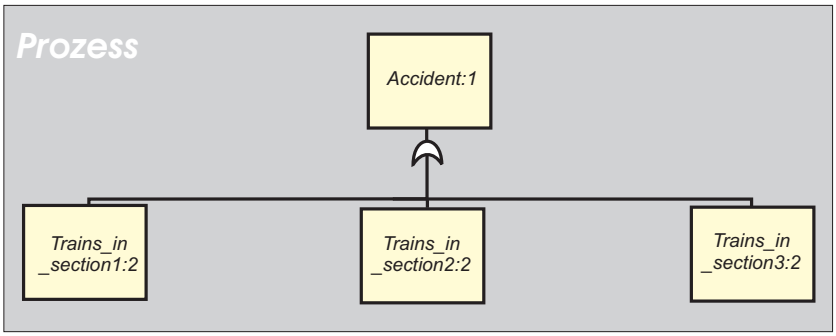

Abbildung 6.3: Unfallbaum des Modells des Eisenbahnbetriebes

Der Unfallbaum des Modells des Eisenbahnbetriebes zeigt übersichtlich alle möglichen betrieblichen Situationen, die zum Zeitpunkt des Auftrittes des unerwünschten Ereignisses vorliegen können. Neben dem Unfallzustand kann der Algorithmus für jede Markierung eines beliebigen Platzes des Petrinetzes angewendet werden und dadurch das Modell (auch während der Modellbildung) verifiziert werden. Zusammen mit dem Graphen von Mengen globaler Zustände bildet der Unfallbaum eine Grundlage zur Modellvalidation im Sinne des Vergleichs mit den Ergebnissen der Gefahrenanalyse (s. Unterkapitel 5.2)

Modellvalidation

Das Ziel der Modellvalidation ist zu prüfen, ob das Modell das tatsächliche Verhalten der modellierten Realwelt beschreibt. Im Rahmen der Modellvalidation ist zu untersuchen

- ob das modellierte Regelverhalten die gleichen Charakteristiken wie die Realwelt aufweist und
- ob das potentielle Fehlverhalten des Modells den Ergebnissen der Gefahrenanalyse (Unterkapitel 5.2) entspricht.

Die Prüfung des Regelverhaltens betrifft vor allem die Art der temporalen und stochastischen Beschreibung ausgedrückt durch die Zeitparameter, Wahrscheinlichkeitsverteilungen, probabilistischen Gewichte oder Arbeitsmodi [Zimmermann 1997] der Transitionen. Außerdem ist auch der Bezug der anderen Netzelemente zur Realität zu prüfen, wie z.B.die Kapazität der Plätze oder die Wichtung der Kanten. Die Grundlage zur Modellvalidation bieten die Ergebnisse quantitativer Analyse des Modells.
Abbildung 6.4 zeigt die durch die stationäre Simulation ermittelten Werte der Zugdichte auf der Beispielstrecke (s. Abbildung 5.7) in Abhängigkeit von der angenommenen Zugfolgezeit (Parameter der Transition *Train-Sequence*). Die einzelnen Messwerte (Züge gesamt, ICE, RB) wurden unabhängig als markierungsabhängige Erwartungswerte des Platzes Trains-in-Block3 ausgewertet. Die ermittelten Werte erfüllen die realistischen Erwartungen.

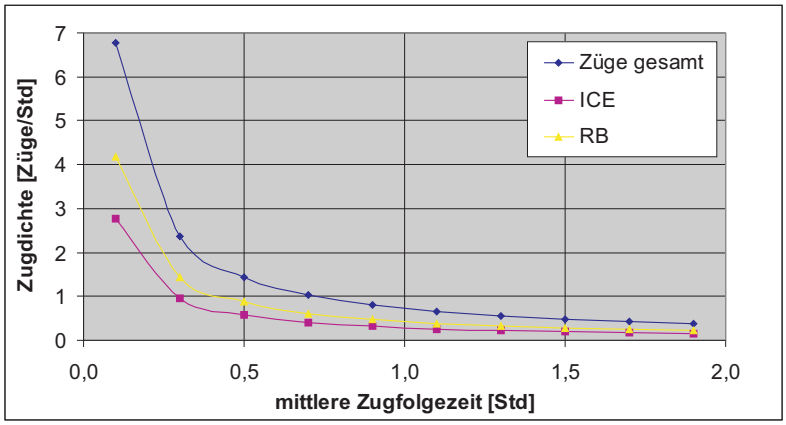

Abbildung 6.4: Abhängigkeit der Zugdichte von der Zugfolge auf der Beispielstrecke

In ähnlicher Weise können auch weitere Charakteristiken des modellierten Betriebsprozesses überprüft werden. Als ein weiteres Beispiel kann die Messung der Fahrzeiten und deren Streuung auf der Gesamtstrecke und auf den einzelnen Streckenabschnitten genannt werden. Die Modellvalidation kann dann auf dem Vergleich mit dem Fahrplan oder mit den realen Fahrzeitdaten basieren.

Die Prüfung des potentiellen Fehlverhaltens basiert auf dem Vergleich des Graphen von Mengen globaler sicherheitsrelevanten Zustände (Abb. 6.2) und des Unfallbaumes (Abb. 6.3) mit den Ergebnissen der vor der Modellierung durchgeführten Gefahrenanalyse.
Der Unfallbaum kann direkt mit einem in der Gefahrenanalyse erstellten Störungsbaum verglichen werden. Ein möglicher Unterschied kann durch unterschiedliche Festlegung

der Abstraktionsebenen (Modelldekomposition) hervorgerufen sein. Dieser ist durch einfache Transformationsalgorithmen bei Bedarf für die Eindeutigkeit der Modellvalidation zu beseitigen.
Die im Graphen von Mengen globaler sicherheitsrelevanter Zustände identifizierten Transitionen entsprechen den Knoten eines Ereignisbaums. Durch geeignete Transformation kann die normkonforme Darstellung des Ereignisbaumes bei Bedarf erzielt werden.

Das Risiko des Eisenbahnbetriebes

Nachdem die Korrektheit und Vollständigkeit der Beschreibung des Eisenbahnbetriebes verifiziert und validiert wurde, kann das Modell zur Auswertung des betrieblichen Risikos herangezogen werden. Da die *PROFUND*-Methode bei der Modellierung des reinen Eisenbahnbetriebes noch nicht den Einfluss der Systemfunktionalität vorsieht, handelt es sich dabei meistens um die Ermittlung eines theoretischen Wertes des vorhandenen Risikos. Obwohl dieser in vielen Fällen nur durch Expertenschätzungen validiert werden kann, ist sein Wert ein wichtiges Ergebnis der Analyse. Seine Bedeutung liegt insbesondere

- als Begründung der Notwendigkeit der Risikoreduktion durch ein Eisenbahnleit- und -sicherungssystem,
- als Basiswert für den Vergleich der Effektivität der Risikoreduktion durch unterschiedliche funktionale oder technische Systemlösungen und
- als Referenzwert zur Sensitivitätsanalyse der Einflüsse von unterschiedlichen Parametern des Eisenbahnbetriebes.

Anderseits kann dieses Modell bei ausreichender Validation des Bezuges zwischen dem Eisenbahnbetrieb und seinen unerwünschten betrieblichen Ereignissen zur Begründung der Überflüssigkeit des Systemseinsatzes im Eisenbahnbetrieb (z.B. mit bestimmten limitierenden Leistungscharakteristiken) verwendet werden.
Die Ergebnisse der Risikoauswertung können direkt in den Graphen von Mengen globaler sicherheitsrelevanter Zustände bzw. in den Unfallbaum eingetragen werden.
Abbildung 6.5 zeigt die Ergebnisse der Risikoauswertung in Abhängigkeit von der mittleren Zugdichte unter Verwendung des Beispielmodells aus der Streckensicherung (Abbildungen 5.5, 5.6 und 5.7). Durch die Kopplung mit dem Modell der Unfallfolgen (Abbildung 5.11) kann der ermittelte Wert der Unfallhäufigkeit (*Kollision* zweier Züge) in das kollektive und in das individuelle Risiko umgerechnet werden (Angenommene Werte: 10 relative Tote pro Unfallsituation, 300 Personen pro Zug, 500-malige Benutzung der Strecke durch ein Individuum pro Jahr z.B. Pendler).

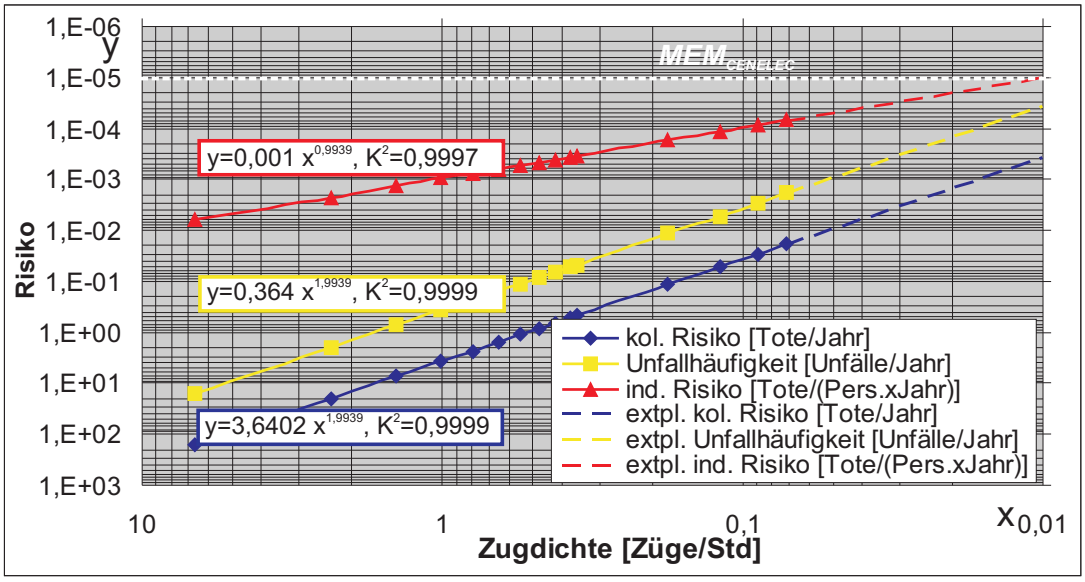

Abbildung 6.5: Risikoauswertung des Modells des Eisenbahnbetriebes in Abhängigkeit von der mittleren Zugdichte bei minimaler Zugfolgezeit von 4 min.

Die durch die Simulation ermittelten Werte zeigen einen linearen bzw. quadratischen Zusammenhang der mit hoher Genauigkeit angenähert werden kann (s. die Näherungsgleichungen mit Korrelationsfaktor $K^2 \approx 1$ in Abb. 6.5). Die funktionale Extrapolation ermöglicht dann die Auswertung von Werten, deren Ermittlung durch Simulation nur in unrealistisch langen Zeiten möglich wäre [Slovák et al. 2005]. Die Werte des individuellen Risikos können mit dem durch die Norm EN 50126 vorgegebenen Akzeptanzwert ($MEM_{CENELEC} = 10^{-5} Tote/(Person \times Jahr)$) verglichen werden.

Die durchgeführte Analyse des Modells des Eisenbahnbetriebes zeigt, dass der Wert des Risikos mit Senkung der Zugdichte nur sehr langsam abnimmt (für die stochastische Beschreibung der Zugfolgezeit einzelner Zugarten wurde eine verschobene Exponentialverteilung angenommen (vgl. Abb.5.9)). Eine wesentlich effektivere Risikoreduktion kann durch Verlängerung der minimalen Zugfolgezeit erreicht werden kann. Abbildung 6.6 veranschaulicht diese Abhängigkeit.

Das ermittelte Risiko kann mit den realen Unfallstatistiken verglichen werden. Im Falle einer relevanten Abweichung von Realwerten sind die Parameter des Modells anzupassen (z.B. Änderung des Verhältnisses zwischen einem Unfall und einem Beinaheunfall, Integration weiterer Risikoreduktionsfaktoren, Berücksichtigung der Züge ohne Beförderung der Personen, usw.) Nach dieser zusätzlichen Validation durch Statistiken kann das Modell des Eisenbahnbetriebes zur Analyse der Einflüsse der Systemfunktionalität und -verlässlichkeit verwendet werden.

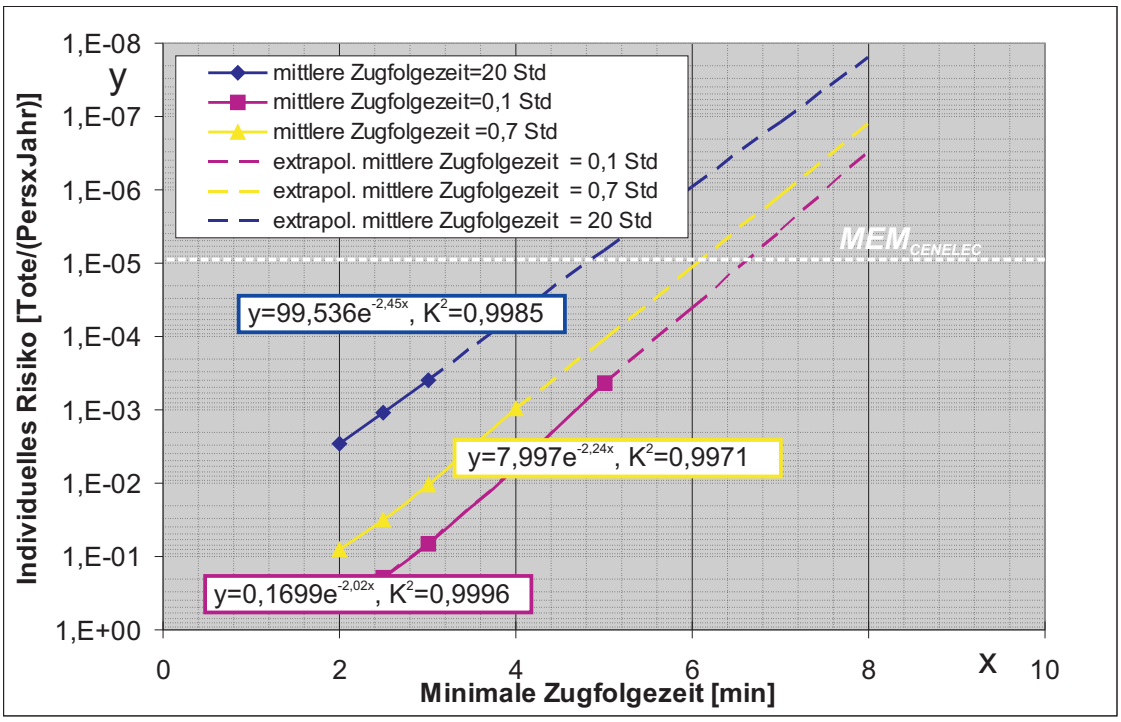

Abbildung 6.6: Abhängigkeit des individuellen Risikos von der minimalen Zugfolgezeit

6.2.2 Analyse des Modells der Systemfunktionalität

Ziel der Analyse des Modells der Systemfunktonalität ist es zu überprüfen, ob die gewählte funktionale Spezifikation des Eisenbahnleit- und -sicherungssystems eine ausreichende Risikoreduktion in dem Eisenbahnbetrieb ermöglicht. Die Aufgabe der Analyse besteht daher wieder in der Modellverifikation, in der durch die Zustandsraumuntersuchung der Ausschluss von unerwünschten Systemzuständen nachgewiesen werden muss, und in der Modellvalidation, in der das modellierte funktionale Verhalten mit dem realen Systemverhalten (oder mit seiner funktionalen Spezifikation) verglichen wird.

Modellverifikation

Die einfachste Art der Modellverifikation ist das interaktive Abspielen der modellierten funktionalen Szenarien und Überprüfung auf die Deadlockfreiheit, sowie auf die Freiheit von unendlichen kausalen oder temporalen Schleifen und auf die Endlichkeit des Zustandraumes (z.B. Vermeidung von endloser Füllung von Plätzen mit Marken) Neben der Generierung des Erreichbarkeitsgraphen bieten die Petrinetze eine Vielzahl von algorithmisch unterstützten Verifikationsmethoden wie Invariantenanalyse, Lebendigkeitsanalyse, Analyse von Traps und Siphons usw. (vgl. 4.1.3).
Abbildung 6.7 zeigt den Erreichbarkeitsgraphen des Eisenbahnbetriebsmodells der Beispielstrecke, das um die Funktionalität der Zugfolgesicherung durch einen einfachen Streckenblock erweitert wurde (aus der Abb. 5.14). Dies ist ersichtlich aus der Markierung der EG-Knoten, die (gegenüber dem EG aus der Abb. 6.1) um den jeweils aktuellen funktionalen Zustand der Zugfolgesicherung (blau hinterlegt) ergänzt wurde. Neben voller Fuktionsfähigkeit der hier modellierten streckenseitigen Zugfolgesicherung setzt das Modell auch die Funktionsfähigkeit der zugseitigen Funktionalität voraus.
Durch die Analyse der Mengen der globalen sicherheitsrelevanten Zustände konnte nachgewiesen werden, dass das modellierte Verhalten weder *Unfallzustände* noch *Gefahrsituationen* enthält. Das ist eine ausreichende Bedingung zur Gewährleistung einer vollen Risikoreduktion durch die Systemfunktionalität im Eisenbahnbetrieb auf der Beispielstrecke.

Modellvalidation

Die Aufgabe der Validation des Modells der Systemfunktionalität besteht darin, durch einen Vergleich des Modellverhaltens mit der Realität oder einer funktionalen Spezifikation seine Korrektheit und die Angemessenheit der gewählten Abstraktion zu prüfen. Wenn das Petrinetzmodell selbst als funktionale Spezifikation dient, oder eine separate (z.B. ausführliche) funktionalen Spezifikation existiert, ist es vorteilhaft die relevanten Eigenschaften des gewünschten funktionalen Verhaltens formal zu beschreiben.

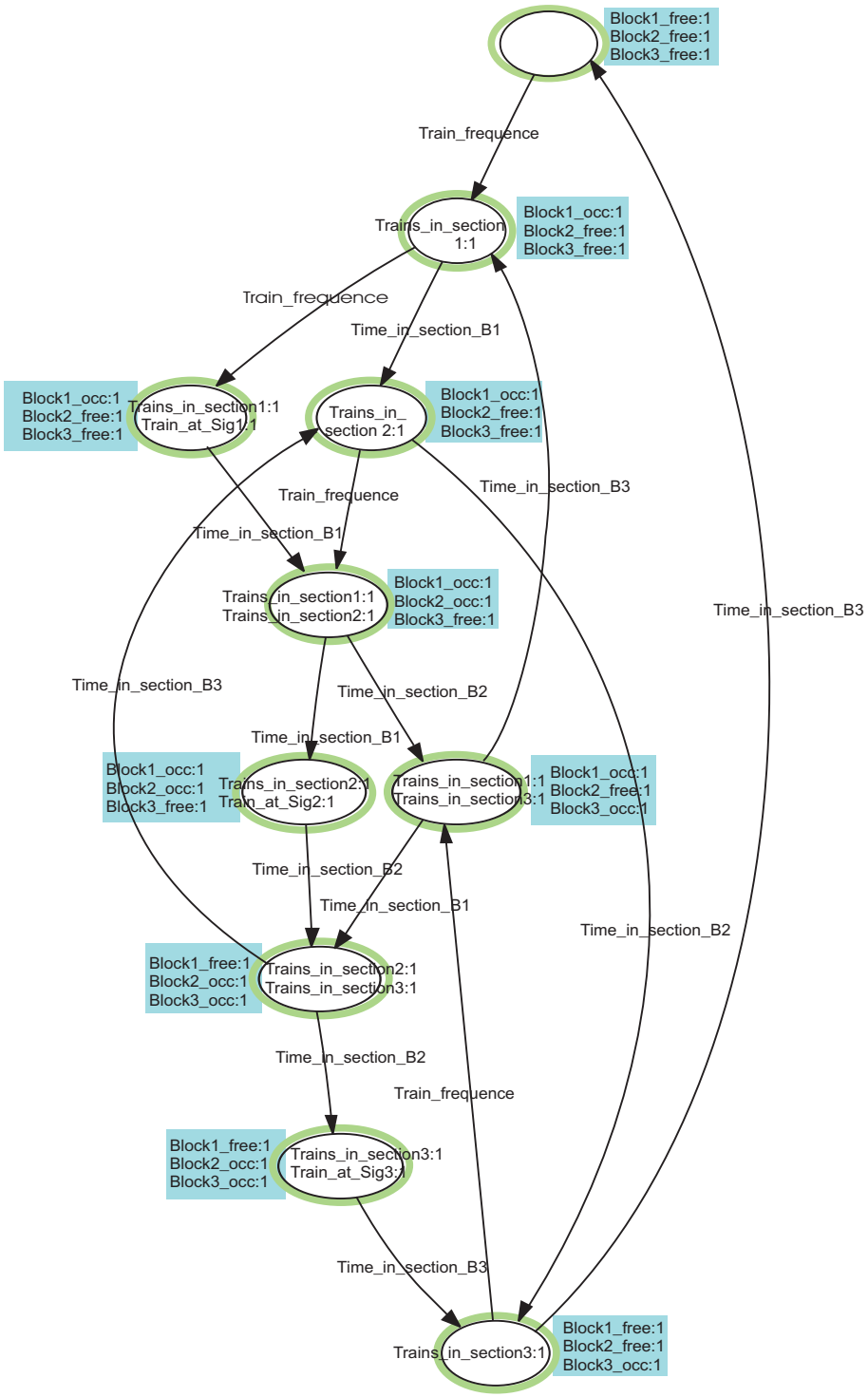

Abbildung 6.7: Erreichbarkeitsgraph des um die Systemfunktionalität erweiterten Modells des Betriebsprozesses

Ein Beispiel der möglichen Formalisierung der qualitiativen funktionalen Sicherheitsanforderungen ist die temporale Logik, die in einer Reihe von Arbeiten insbesondere aus dem Bereich Softwarespezifikation in Verbindung mit einem *Model Checking* verwendet wurde [Ehrig 2004] [Ortmeier 2005]. Eine andere Möglichkeit bietet eine natürlichsprachliche Formulierung der Sicherheitsanforderungen in Form der *Safety Patterns* [Bitsch et al. 2004].
Für die Funktionalität der als Beispiel genommenen Streckensicherung lassen sich z.B. die Exklusivität der Markierung der Plätze *Block1-free* und *Block1-occ* usw. oder Anforderung ständig gleichzeitiger Markiertheit der Plätze *Trains-in-section1* und *Block1-occ* oder *Train-at-Sig1* und *Block1-occ*, usw. als qualitative funktionale Sicherheitsanforderungen formulieren. Diese können direkt durch Analyse der Markierungen der Knoten des Erreichbarkeitsgraphen (Abb. 6.7) überprüft werden.

Das Risiko der Systemfunktionalität

Durch die Analyse des Modells der Systemfunktionalität muss gezeigt werden, dass die durch die entsprechende funktionale Spezifikation gewährleistete Risikoreduktion für einen normkonform sicheren Eisenbahnbetrieb ausreicht. Durch die konzeptuelle Verbindung der Systemfunktionalität mit dem Eisenbahnbetrieb im Sinne der *PROFUND*-Methode und dank der Kopplung mit dem Modell der Unfallfolgen ist es möglich, jederzeit das Risiko der funktionalen Systemlösung R_F durch numerische Analysen oder Simulationen auszuwerten. Das Ergebnis der Auswertung kann zu folgenden Arten des weiteren Vorgehens führen:

- $R_F = 0$ oder $R_F < R_{tolerable}$: Kein Restrisiko (muss auch durch Modellverifikation bestätigt werden) bzw. ein akzeptierbares Restrisiko funktionaler Spezifikation. Das Restrisiko kann aber nur unter Vorbehalt der Ergebnisse der Verlässlichkeitsanalyse akzeptiert werden. Falls diese Lösung zu unrealisierbaren funktionalen Verlässlichkeitsanforderungen führt (s. Kap. 6.2.3) ist ein funktionales Re-design notwendig.

- $R_F > R_{tolerable}$: Unakzeptierbares Restrisiko führt zu einem unumgänglichen funktionalen Re-design.

Das als Beispiel betrachtete funktionale Modell der Zugfolgesicherung zeigt bei seiner angenommenen vollständigen Funktionsfähigkeit eine vollständige Risikoreduktion.
Als Beispiel einer funktionalen Spezifikation mit unvollständiger Risikoreduktion können z.B. einige funktionale Lösungen der Bahnübergangsicherung genannt werden, deren Restrisiko von bahnexternen Faktoren (hier menschlicher Faktor des KFZ-Fahrers) abhängig ist (nähere Analyse des Bahnübergangsbeispiels im Unterkapitel 7.4.2).

Über die endgültige Akzeptanz der funktionalen Spezifikation entscheiden die Analyseergebnisse des Modells der Systemfunktionsverlässlichkeit.

6.2.3 Analyse des Modells der Systemfunktionsverlässlichkeit

Die Aufgabe der Analyse des Modells der Systemfunktionsverlässlichkeit ist es, für die durch das Modell der Systemfunktionalität repräsentierte funktionale Spezifikation die quantitativen Sicherheitsziele zu definieren. Gegendstand der Betrachtung sind dabei alle modellierten funktionalen Ressourcen, die für die Durchführung der sicherheitsrelevanten Systemfunktionen zuständig sind. Die Festlegung der quantitativen funktionalen Sicherheitsziele basiert auf der Auswertung des Risikos unter Betrachtung der Verlässlichkeitseigenschaften der sicherheitsrelevanten Funktionsressourcen.
Ein mögliches Vorgehen dabei ist, bestimmte Verlässlichkeitseigenschaften (wie z.B. Ausfallraten, Wartungs- und Offenbarungsintervalle, Reparaturzeiten usw.) der Ressourcen anzunehmen (z.B. auf Erfahrungsbasis) und durch Analyse des Modells deren Akzeptanz positiv oder negativ zu beurteilen. Eine positive Beurteilung kann dann erbracht werden, wenn das ausgewertete Restrisiko im Eisenbahnbetrieb unterhalb der gesetzlichen Akzeptanzgrenze liegt. In diesem Falle können dann die angenommenen Verlässlichkeitseigenschaften als Sicherheitsziele definiert und als Ergebnisse der Analyse deklariert werden.
Ein anderes Vorgehen geht nicht von bestimmten Verlässlichkeitseigenschaften der Ressourcen aus, sondern benutzt das Modell der Systemfunktionsverlässlichkeit um die optimale Sicherheitsziele herauszufinden. Im Allgemeinen soll das Optimierungsziel im Erreichen der niedrigstmöglichsten Life-Cycle-Kosten liegen (insbesondere Herstellung und Betrieb). Einfachstes Kriterium der Optimierung kann die Bestrebung sein, die höchstmöglichen Grenzen der Verlässlichkeitsparameter (bei deren negativer Auswirkung auf die Sicherheit, sonst gilt das Gegenteil) zu ermitteln. Bei Zugänglichkeit der Kostenfunktionen kann daher die Optimierung präzisiert werden und als Sicherheitsziele die global kosteneffektivsten Verlässlichkeitsparameter der Ressourcen deklariert werden.
Wie bei der Analyse vorheriger Modelltypen ist vor der eigentlichen Evaluation des Restrisikos im Eisenbahnbetrieb auch das Modell der Funktionsverlässlichkeit zu verifizieren und zu validieren.

Modellverifikation

Neben den bereits im Kapitel 6.2.1 erwähnten Methoden der Modellverifikation wie Syntax check, Analyse der Lebendigkeit anhand des Erreichbarkeitsgraphen, Entdeckung

endloser Schleifen, interaktives Abspielen der Schaltsequenzen (Markenspiel) usw. ist an dieser Stelle die Invariantenanalyse zu erwähnen.

Invariantenanalyse Im Falle der Analyse der P-Invarianten (s. Unterkap. 4.1.3) kommen als Ergebnis die Mengen der Plätze heraus. Die gewichtete Tokensumme, die durch diese Plätze durchfließt, bleibt innerhalb der erreichbaren Zuständen konstant. Die Invariantenanalyse führt daher zur Identifikation von zyklisch verbundenen lokalen Zustandsfolgen, so, wie sie in der Modellierung der Systemfunktionalität (bei Modellierung aller Funktionen auf Aufforderung, s. Unterkap. 5.4.1) zu finden ist.
Das Ergebnis der P-Invariantenanalyse muss also bestätigen, dass alle Plätze der funktionalen Modellierung, die der Modellierung der Funktionen auf Aufforderung (die Funktionen im Dauerbetrieb werden ja statisch modelliert) zugehören, jeweils mindestens durch eine P-Invariante abgedeckt sind. P-Invarianten können somit zur intuitiven Validation dienen - findet sich für einen erwarteten modellierten Zyklus keine P-Invariante, dann ist eine genauere Untersuchung ratsam. Ausserdem kann durch Ermittlung der maximalen Markiertheit eines in einer P-Invariante enthaltenen Platzes der Ausschluss von verbotenen oder unerwünschten Systemzuständen (z.B. Unfallzustände) nachgewiesen werden.
Unter Einhaltung der in Kapitel 4 vorgestellten Modellierungsmethodik soll es nie zu einem Markenaustausch zwischen den einzelnen Betrachtungsebenen (Prozess, Funktionalität, Verlässlichkeit) kommen. Da die gegenseitige Beeinflussung nur durch Abfragekanten oder Inhibitoren beschrieben ist, darf auch keine minimale P- und keine minimale T-Invariante (minimale Invarianten sind solche, die keine anderen Invarianten als Teilmengen enthalten) Grenzen einer Betrachtungsebene überschreiten. Falls die Invariantenanalyse ein anderes Ergebnis zeigt, deutet dieses einen signifikanten Fehler in der Modellierung an.
Eine weitere Aussage zur Korrektheit der Modellierung bringt die erreichbarkeitsgraphbasierte Konstruktion des Graphen von Mengen globaler sicherheitsrelevanter Zustände und des Unfallbaumes.

Graph von Mengen globaler sicherheitsrelevanter Zustände In der Regel folgen die unerwünschten Ereignisse im Betrieb aus Hazardzuständen der funktionalen Ressourcen. Deswegen muss auch das modellierte Verhalten diese kausale Folge aufweisen. Im Unterkapitel 6.2.1 wurden die Mengen der globalen sicherheitsrelevanten Zustände U, GS und RV definiert. Im Sinne der genannten kausalen Folge kann die Menge eines globalen Hazardzustandes als Untermenge der Menge RV wie folgt definiert werden:

$$H := \{m \in RS | m(H\text{-}Platz) = 1\} \subseteq RV \tag{6.6}$$

wobei als *H-Platz* der Platz des gefährlichen Ausfalles (Hazards) eines Verlässlichkeitsmodells der zugehörigen Funktionsressource bezeichnet wird und $m(H\text{-}Platz) = 1$ die Menge aller Markierungen (Zustände) mit einem solchen markierten *H-Platz* repräsentiert.
Der Erreichbarkeitsgraph des Prozess-Funktionsverlässlichkeitsmodells des Beispieles aus der Streckensicherung (Abb. 5.24) besteht aus 6830 zeitbehafteten Knoten, daher ist seine Darstellung und visuelle Analyse nicht mehr praktisch durchführbar. Abbildung 6.8 zeigt den Graph der globalen sicherheitsrelevanten Zustandsmengen im Sinne der vorherigen Definition der *U*, *GS*, *RV* und *H* Mengen mit Angabe der zugehörigen Anzahl der EG-Knoten.

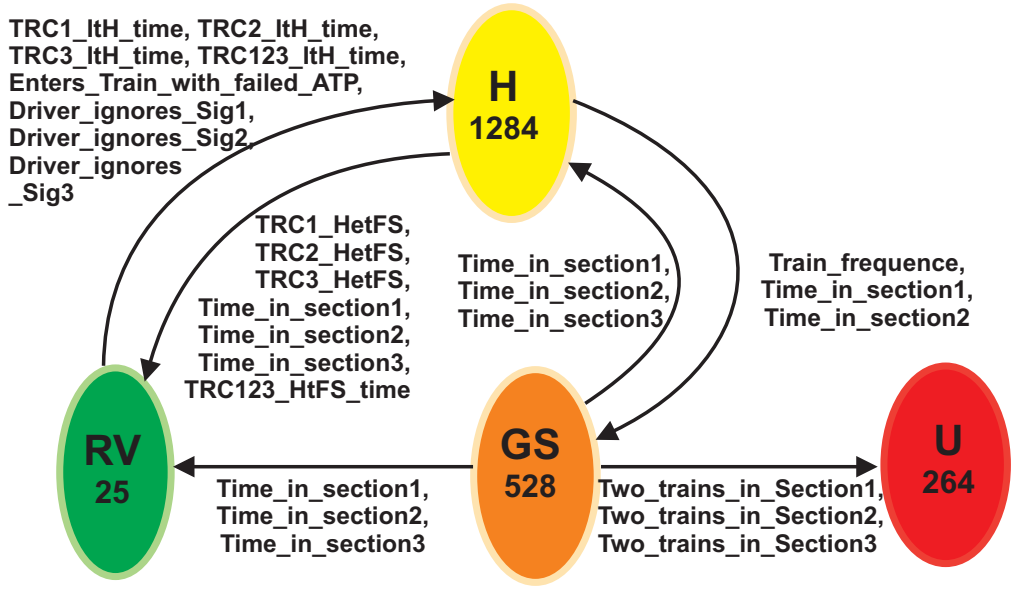

Abbildung 6.8: Graph von Mengen globaler sicherheitsrelevanter Zustände des Prozessfunktions-verlässlichkeitsmodells

Die erhaltene Zustandsfolge entspricht dem erwarteten Ablauf, und die genaue Analyse der Übergangstransitionen bildet die Basis detaillierter Modellverifikation.

Unfallbaum Das Ziel des im Unterkapitel 6.2.1 eingeführten Unfallbaums war es, alle Betriebssituationen (globale Modellzustände) zu identifizieren, in der ein bestimmter Zustand des Modellverhaltens erreicht werden kann. Durch Erweiterung des Modells um die Systemfunktionalität und Systemfunktionsverlässlichkeit erweitert sich entsprechend auch die Anzahl der verschiedenen Untermengen der globalen Menge des Unfallzustandes. Aus der Sicht des Unfallbaumes sind neben den lokalen Zuständen im Betriebsprozess (repräsentiert durch die in dem Unterkap. 6.2.1 genannten *P-Plätze*

bzw. *PP-Plätze*, usw.) von besonderer Wichtigkeit die lokalen Modellzustände die das potenzielle Fehlerverhalten der Systemfunktionalität beschreiben. Diese kann man als *V-Plätze* bezeichnen, da sie die grundlegenden Verlässlichkeitszustände der sicherheitsrelevanten Funktionsressourcen beschreiben (s. Abb. 5.19).
Wie im Unterkapitel 5.4.2 beschrieben ist, werden die grundlegenden Verlässlichkeitszustände nach unterschiedlichen Hazardverlaufsarten im Sinne der Abbildungen 5.20 (für eine hazard-aktive Funktion) und 5.21 (für eine hazard-passive Funktion) verfeinert. Die einzelnen Hazardverlaufsarten repräsentierenden Plätze, die *H-Plätze* (wie z.B *HeI-state*, *HtFS-state*, usw.) stellen grundsätzlich die unterste Abstraktionsebene der Funktionsverlässlichkeitsmodellierung dar. Da die *H-Plätze* für die genaue Ursachen des Fehlverhaltens der Systemfunktionalität und der unerwünschten Ereignisse in dem Betriebsprozess stehen, ist das Herausfinden der gegenseitigen Beziehung ein grundsätzliches Ziel der Analyse.
Die Plätze jeder weiteren Abstraktionsebene zwischen den *V-* und *H-Plätzen* können als *VV-Plätze* (bzw. *VVV-Plätze*, usw.) bezeichnet werden.
Tabelle 6.3 zeigt die sicherheitsrelevanten Plätze der EG-Knoten der globalen Menge des Unfallzustandes des Funktionsverlässlichkeitsmodells des Beispieles aus der Streckensicherung (Abb. 5.24). Im Vergleich mit der entsprechenden Tabelle des Modells des Eisenbahnbetriebes (Abb. 6.2) ist durch die Einführung der Signale das Prozessmodell um eine weitere Abstraktionsebene verfeinert worden (*PP-Plätze*). Außerdem finden sich in der Tabelle die zwei Abstraktionsebenen des Funktionsverlässlichkeitsmodells wieder (*V-* und *H-Plätze*).

Beschr.Nr.	U	P	PP	V	H
1	Accident:1	Trains_in_Section1:2	Trains_in_Block1:2	TRC_hazard:>0;	TRC_hazard:trc1
2		Trains_in_Section2:2	Trains_in_Block2:2	TP_failed_Sig1:1;	Driver_SPAD_Sig1:1
3		Trains_in_Section3:2	Trains_in_Block3:2	TP_failed_Sig2:1;	Trains_with_failed_ATP:>0
4			Trains_at_Sig1:2	TP_failed_Sig3:1;	TRC_hazard:trc123
5			Trains_at_Sig2:2		Driver_SPAD_Sig2:1
6			Trains_at_Sig3:2		TRC_hazard:trc2
7					Driver_SPAD_Sig3:1
8					TRC_hazard:trc3

Tabelle 6.3: Die sicherheitsrelevanten Plätze der EG-Knoten der globalen Menge des Unfallzustandes des Prozess-Funktionsverlässlichkeitsmodells

Ebenso wie in Abbildung 6.2 könnten die Markierungen aller Knoten des globalen Unfallzustandes aufgeführt werden, wobei jede Spalte einem Platz der möglichen Markierung entsprechen würde (hier wären es neben dem *U-Platz* 4 weitere Platzgruppen: 3 *P-Plätze*, 6 *PP-Plätze*, 4 *V-Plätze* und 8 *H-Plätze*). Durch die konsekutive Analyse der jeweils nebeneinander stehenden Platzgruppen (startend von dem *U-Platz* und

der *P-Gruppe* bis hin zur Analyse der *V-Gruppe* mit der *H-Gruppe* konnten die in Abbildung 6.9 aufgeführten Gleichungen ermittelt werden.
Die Gleichungen ordnen einem Platz der höheren Abstraktionsebene die möglichen Kombinationen von markierten Plätzen der unteren Ebene zu. Die logischen Ausdrücke UND (*), ODER (+) geben an, ob bestimmte markierte Plätze in der Markierung eines EG Knoten des globalen Unfallzustandes immer gleichzeitig vorkommen (UND) oder sie auch einzeln auftreten (ODER) können, wobei alle anderen Plätze unmarkiert bleiben. Im Falle einer Feststellung eines Einzelauftrittes der Markierung bestimmter Plätze ist die Aufführung möglichst vorher festgestellter gleichzeitiger Markierung aus der Sicherheitsbetrachtung irrelevant. Diese entspricht dem Fall, wenn der Unfall in einer Situation, in der zwei oder mehrere Bedingungen gleichzeitig erfüllt sind, passiert, jedoch auch die Erfüllung einer einzelnen Bedingung schon ausreichend ist, um den Unfall zu verursachen.
Die Gleichungen der Beziehungen zwischen den Gruppen der Plätze der EG-Knoten des globalen Unfallzustandes können durch Verwendung der Semantik der Störungsbäume zum Aufbau eines Unfallbaumes des Prozess-Funktionsverlässlichkeitsmodells verwendet werden. Abbildung 6.10 stellt einen Ausschnitt aus dem Unfallbaum des Beispieles aus der Streckensicherung dar.
Der Unfallbaum deutet übersichtlich an, welche sicherheitsrelevanten Plätze mit der Markierung des Unfallplatzes gleichzeitig markiert werden können. Die Integration weiterer Einzelplätze oder Gruppen der Plätze (z.B. der *F-Plätze*) kann eine detaillierte Aussage zur möglichen Gesamtmarkierung des Unfallzustandes bringen, ohne den gesamten Erreichbarkeitsgraphen des Modells direkt analysieren zu müssen.
Neben dem Unfallzustand kann auch jeder andere Platz ähnlich analysiert werden. Die Bedingung der Anwendung ist eine Voraussetzung dafür, dass nach dem Auftritt der untersuchten Platzbelegung alle Transitionen an ihrem weiteren Schalten verhindert werden und der untersuchte Modellzustand eine so genannte absorbierende Markierung des Netzes darstellt (so wie im Falle der Belegung eines Unfallplatzes).
Die integrierte Betrachtung aller Abstraktionsebenen des Modells ermöglicht, den Unfallbaum effektiv bei der Modellverifikation anzuwenden.

Modellvalidation

Die Aufgabe der Modellvalidation eines Modells der Prozess-Funktions-Verlässlichkeit ist, zu überprüfen, ob das modellierte Verlässlichkeitsverhalten der sicherheitsrelevanten Funktionsressourcen die der Gefahrenanalyse (s. Unterkap. 5.2) entsprechende Auswirkung auf den Eisenbahnbetrieb aufweist.
Zu diesem Zweck kann das interaktive Durchspielen der betrieblichen Szenarien unter verschiedenen Verlässlichkeitszuständen der Ressourcen angewendet werden. Eine

U-Platz	*P-Gruppe*
U1=	P1 + P2 + P3
P-Gruppe	*PP-Gruppe*
P1=	P1PP1 + P1PP4
P2=	P2PP2 + P2PP5
P3=	P3PP3 + P3PP6
PP-Gruppe	*V-Gruppe*
P1PP1=	P1PP1V1 + P1PP1V2
P1PP4=	P1PP4V1 + P1PP4V2
P2PP2=	P2PP2V1 + P2PP2V3
P2PP5=	P2PP5V1 + P2PP5V3
P3PP3=	P3PP3V1 + P3PP3V4
P3PP6=	P3PP6V1 + P3PP6V4
V-Gruppe	*H-Gruppe*
P1PP1V1=	P1PP1V1H1 + P1PP1V1H4
P1PP1V2=	P1PP1V2H2 * P1PP1V2H3
P1PP4V1=	P1PP4V1H1 + P1PP4V1H4
P1PP4V2=	P1PP4V2H2 * P1PP4V2H3
P2PP2V1=	P2PP2V1H4 + P2PP2V1H6
P2PP2V3=	P2PP2V3H5 * P2PP2V3H3
P2PP5V1=	P2PP5V1H4 + P2PP5V1H6
P2PP5V3=	P2PP5V3H5 * P2PP5V3H3
P3PP3V1=	P3PP3V1H4 + P3PP3V1H8
P3PP3V4=	P3PP3V4H7 * P3PP3V4H3
P3PP6V1=	P3PP6V1H4 + P3PP6V1H8
P3PP6V4=	P3PP6V4H7 * P3PP6V4H3

Abbildung 6.9: Beziehungen zwischen den Plätzen des globalen Unfallzustandes

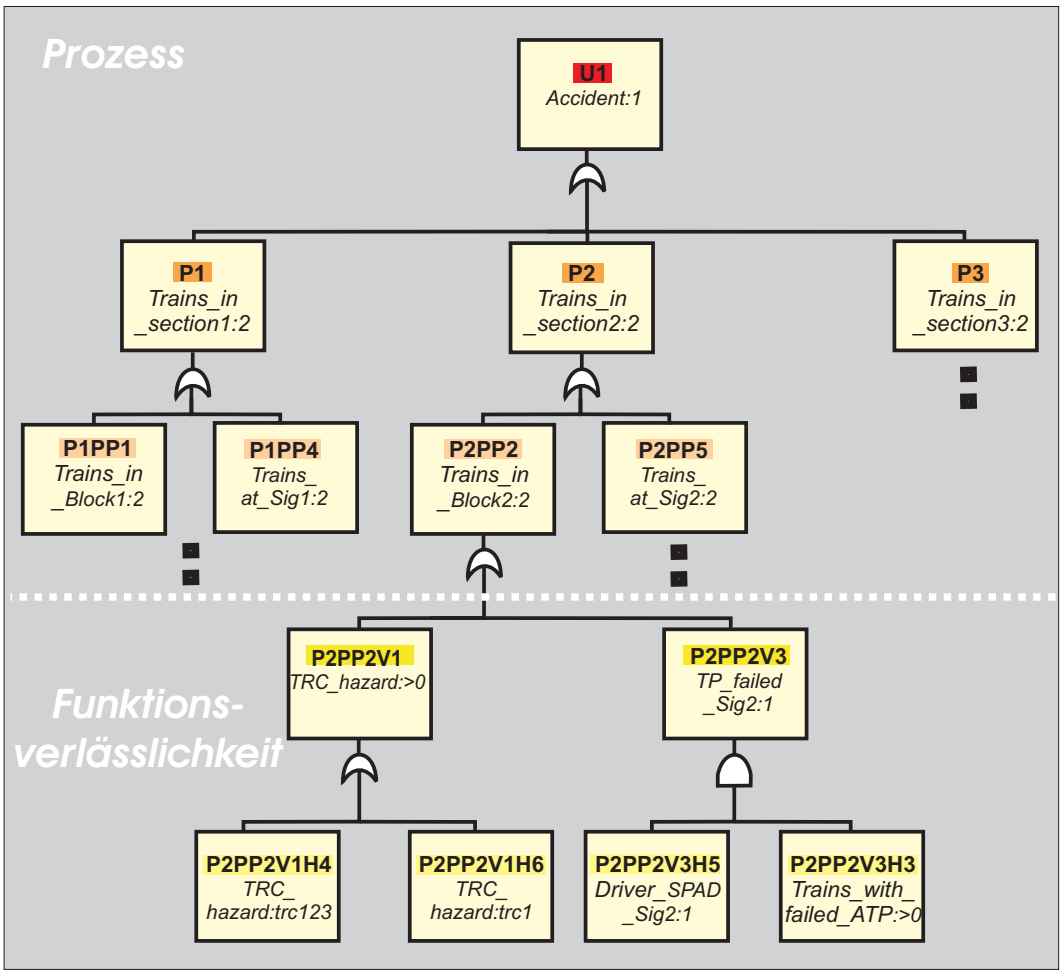

Abbildung 6.10: Unfallbaum des Beispieles aus der Streckensicherung (Ausschnitt)

Zeitersparnis bei der interaktiven Validation des Modells bietet die Möglichkeit, das Modell in einen konkreten Zustand zu bringen und von dort aus die Untersuchungen des Verhaltens zu beginnen. Um jedoch zu gewährleisten, dass bei manuellem Versetzen in einen Ausgangszustand nicht eine unerreichbare Markierung eingegeben wird, ist ein dynamischer Abgleich mit dem Erreichbarkeitsgraphen des Modells sehr vorteilhaft.

Unfallbaum Eine weitere Validationsmöglichkeit des Modells bietet der berechnete Unfallbaum, der mit dem Störungsbaum der vor der Modellierung durchgeführten Gefahrenanalyse (Abb. 5.3) verglichen werden kann. Der in Abbildung 6.10 dargestellte Unfallbaum des Prozess-Funktions-Verlässlichkeitsmodells zeigt detailliert an, welche gefährlichen Fehlzustände (Hazards) in der Systemfunktionalität zu einem Unfall (Kollision) im Streckenblock 2 führen können. Dieses kann einerseits (streckenseitig) der Totalausfall der Streckenblocksicherung oder ein lokaler Ausfall der Sicherung des zweiten Blocks sein, anderseits (zugseitig) könnte ein Lokführerfehler (Vorbeifahrt an einem haltzeigenden Signal) mit einem gleichzeitigen Ausfall der Zugsicherung zum Unfall führen.

Graph von Mengen globaler Zustände Die im Rahmen der Analyse der Beziehungen unter den möglichen Markierungen der EG-Knoten des globalen Unfallzustandes im Sinne der Gleichungen aus Abbildung 6.9 können bei der Verfeinerung des Graphen der globalen sicherheitsrelevanten Zustandsmengen verwendet werden. Abbildung 6.11 zeigt einen solchen aus dem Modell der Beispielstrecke ermittelten Graphen (angezeigt sind nur die zum Unfall führenden Zustandsübergängen), in dem einerseits der globale Zustand der gefährlicher Situationen (GS) und anderseits der globale Hazardzustand (H) verfeinert wurden .

Der globale Zustand der gefährlichen Situationen wurde entsprechend dem Auftritt der *P-Plätze* (*P1*, *P2* und *P3* - s. Abb. 6.3) in drei Unterzustände untergeteilt (*GS1*, *GS2* und *GS3*). Ebenso wurde der globale Hazardzustand nach den *H-Plätzen* verfeinert (*H1* bis *H8*), wobei neben dem Einzelauftritt ein globaler Unterzustand auch jeder durch logische Verbindung AND verknüpften Kombination der *H-Plätze* globaler Unterzustand zugeordnet wurde (*H2H3*, *H3H5* und *H3H7*).

Durch eine weitere Analyse des Erreichbarkeitsgraphen können die Transitionen aller Übergänge zwischen zwei beliebigen globalen Mengen ermittelt werden. Diese entsprechen den sicherheitsrelevanten Ereignissen des Modellverhaltens und bilden eine Grundlage zur Validation durch den Vergleich mit einem Ereignisbaum, der vor der Modellierung im Rahmen der Gefahrenanalyse erstellt wurde.

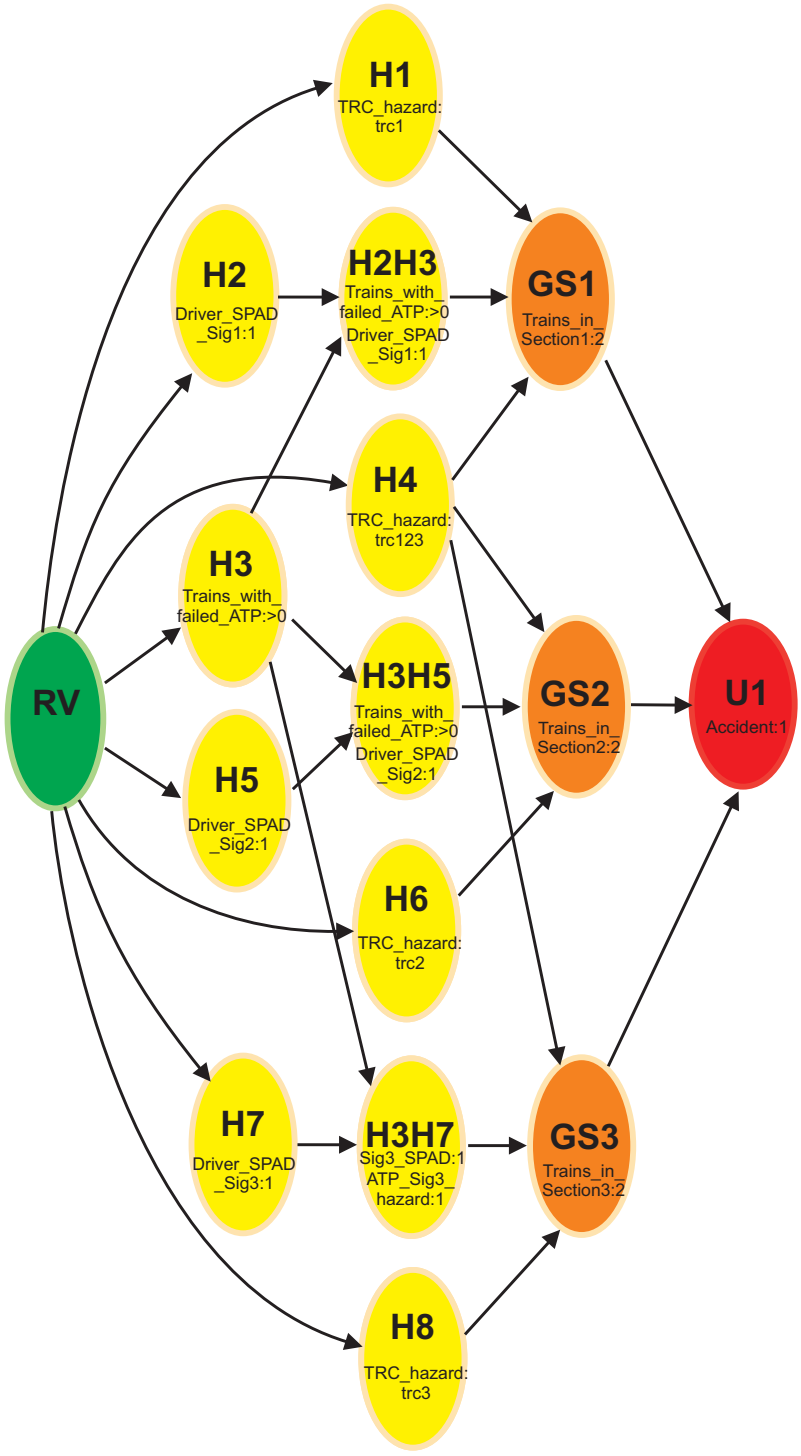

Abbildung 6.11: Verfeinerter Graph globaler Zustandsmengen des Beispiels aus der Streckensicherung (nur zum Unfall führende Zustandsübergänge dargestellt)

Das Risiko der Systemfunktionsverlässlichkeit

Unter der Voraussetzung, dass durch die Risikoauswertung des prozess-funktionalen Modells die notwendige Risikoreduktion nachgewiesen werden kann, soll das Modell der Systemfunktionsverlässlichkeit dazu verwendet werden, den Einfluss der Verlässlichkeitsparameter der betrachteten funktionalen Ressourcen auf das resultierende Risiko im Eisenbahnbetrieb zu untersuchen. Ziel dieser Untersuchung ist, die Bedingungen zur optimalen Bestimmung der Grenzwerte der Verlässlichkeitsparameter zu schaffen, die das akzeptierbare Risiko des Eisenbahnbetriebs garantieren würden.
Das Modell der Systemfunktionsverlässlichkeit zusammen mit dem Modell des Eisenbahnbetriebs und der Unfallfolgen erlaubt direkt die Überprüfung, ob bestimmte angenommene Werte der Verlässlichkeitsparameter der Ressourcen der sicherheitsrelevanten Systemfunktionen die notwendige Risikoreduktion im Eisenbahnbetrieb ermöglichen. Ein solches Ergebnis könnte dazu genutzt werden, die quantitativen Sicherheitsanforderungen an die Ressource zu formulieren, sagt aber nichts über ihre Optimalität aus. Eine optimale Definition der Sicherheitsanforderungen kann nur auf der Basis einer Sensitivitätsanalyse aufgebaut werden.

Sensitivitätsanalyse Die Aufgabe einer Sensitivitätsanalyse ist es, den Einfluss einzelner lokaler Verlässlichkeitsparameter auf die globalen Verlässlichkeitseigenschaften des Modells genau zu untersuchen. Im Falle der hier behandelten bahnspezifischen Anwendung, in der das betriebliche Risiko als globale Modelleigenschaft ausgewertet wird, betrifft die Sensitivitätsanalyse das Einflusspotential der Verlässlichkeitsparameter aller sicherheitsrelevanten funktionalen Ressourcen, d.h. Ressourcen der Systemfunktionen, die direkt oder indirekt das resultierende betriebliche Risiko beeinflussen können, wobei

- als *direkt risikobeeinflussende funktionale Ressourcen* die Ressourcen bezeichnet werden können, deren Ausfallverhalten direkt ohne Abhängigkeit von anderen funktionalen Ressourcen für einen unzulässigen Anstieg des Risikos im Eisenbahnbetrieb verantwortlich sein kann und

- die *indirekt risikobeeinflussenden funktionalen Ressourcen* das Betriebsrisiko nur im Zusammenhang mit dem Ausfällen anderer sicherheitsrelevanter Ressourcen oder Faktoren (z.B. Mensch) negativ beeinflussen können.

Eine eindeutige Unterteilung in direkt und indirekt risikobeeinflussende funktionale Ressourcen im Modell bietet der zur Modellverifikation aufgebaute Unfallbaum. Das Fehlerverhalten der sicherheitsrelevanten Ressourcen ist im Unfallbaum durch die unterste Ebene der *H-Plätze* repräsentiert. Alle *H-Plätze* der untersten Ebene eines Unfallbaumes, die mit dem Top-Zustand (Unfall) ausschließlich durch OR-Gatter verbunden

sind, gehören zu den *direkt risikobeeinflussenden funktionalen Ressourcen. H-Plätze*, die innerhalb der Verbindung zu dem Top-Zustand mindestens ein AND-Gatter haben, gehören andererseits zu den *indirekt risikobeeinflussenden funktionalen Ressourcen.*
Der erste Schritt der Sensitivitätsanalyse betrifft die Analyse der Einflüsse der Verlässlichkeitsparameter der direkt risikobeeinflussenden funktionalen Ressourcen $i_1..i_M$, wobei alle mit einem AND-Gatter verbundenen indirekt risikobeeinflussenden funktionalen Ressourcen $j_1..j_N$ in diesem Schritt in eine Gruppe zusammenzufassen sind und so als eine direkt risikobeeinflussende funktionale Ressource zu betrachten sind.
Dazu ist es notwendig, bei *N-1* indirekt risikobeeinflussenden funktionalen Ressourcen, die in einer Gruppe zusammengefasst sind, zuerst bestimmte Verlässlichkeitswerte anzunehmen, wobei entweder mittlere Werte aus dem vorgesehenen Wertebereich (z.B. bei Ausfallraten der Funktionsressourcen) oder maximale Werte mit negativer Risikoauswirkung (z.B. das ungünstigste menschliche Verhalten) zu Grunde gelegt werden können. Für das weitere Vorgehen ist es sinnvoll, bei solchen indirekt risikobeeinflussenden Ressourcen die Verlässlichkeitsparameter festzulegen, deren Variation nicht vorgesehen ist (z.B. Parameter menschlichen Verhaltens) oder Ressourcen, bei denen kein großer Einfluss auf die Life-Cycle-Kosten zu erwarten ist. Diese Parameterannahme ist bei allen Gruppen anzuwenden.
Die Aufgabe der Analyse besteht dann darin, den möglichen Einfluss jeder einzelnen direkt risikobeeinflussenden funktionalen Ressource $i\epsilon\{1..M\}$ (bzw. auch jeder zu einer direkt risikobeeinflussende Ressource betrachtete Gruppe indirekt risikobeeinflussender Ressourcen) auf das betriebliche Risiko zu evaluieren. Dabei ist jeweils der Einfluss aller anderen Ressourcen zu unterdrücken (z.B. deren Hazardausfälle nicht zuzulassen). Das Ergebnis sind Ressourcen-spezifische *Risikocharakteristiken* R_i als Näherungsfunktionen des entsprechenden Verlässlichkeitsparameters p_i:

$$R_i = R_V + R_F, i\epsilon\{1..M\} \tag{6.7}$$

wobei R_F das funktionale Restrisiko (s. Unterkap. 6.2.2) darstellt.
Die unfallbaumbasierte Ermittlung der direkten risikobeeinflussenden funktionalen Ressourcen ermöglicht, die Unabhängigkeit derer Verlässlichkeitsparameter anzunehmen. Daher kann das resultierende betriebliche Risiko der Systemfunktionsverlässlichkeit R_V durch Addition der Risikobeiträge einzelner direkt risikobeeinflussender Ressourcen ausgewertet werden.

$$R_V = \sum_{i=1}^{M} R_i(p_i) \tag{6.8}$$

Das resultierende Risiko des Eisenbahnbetriebes besteht dann aus dem Risiko der Funktionsverlässlichkeit R_V und dem funktionalen Restrisiko R_F.

$$R = R_V + R_F = \sum_{i=1}^{M} R_i(p_i) + R_F = R_V(\overrightarrow{p}) + R_F \tag{6.9}$$

Dabei ist der Vektor $\overrightarrow{p}$ ein Vektor aller konkreter Werte a der Verlässlichkeitsparameter der direkten bzw. indirekten risikobeeinflussenden funktionalen Ressourcen.
Für ein bestimmtes *PROFUND*-Modell ist ein Vektor $\overrightarrow{p}$

- *akzeptierbar* wenn das resultierende Risiko des Eisenbahnbetriebs gleich oder kleiner als das durch die Norm vorgeschriebene maximale Restrisiko ist.

$$R = R_F + R_V(\overrightarrow{p_{acceptable}}) \leq R_{tolerable} \tag{6.10}$$

- *kostenoptimal* wenn das resultierende Risiko des Eisenbahnbetriebs dem durch die Norm vorgeschriebenen maximalen Restrisiko entspricht (bzw. unter diesem Wert liegt) und die Gesamtsumme der Life-Cycle-Kosten aller beteiligten funktionalen Ressourcen das Minimum erreicht.

$$R = R_F + R_V(\overrightarrow{p_{costoptimal}}) \leq R_{tolerable}, \tag{6.11}$$

$$\sum_{i=1}^{M} C_i(p_i) \longrightarrow min,$$

  wobei $C_i(p_i)$ eine Kostenfunktion der funktionalen Ressource i in Abhängigkeit von dem Verlässlichkeitsparameter p_i ist.

Ein akzeptierbarer Vektor $\overrightarrow{p_{acceptable}}$ kann durch einfache Auswertung der Gleichung 6.9 herausgefunden werden. Da die Kostenfunktionen der Ressourcen meistens nicht lineare Funktionen sind (oft nur als diskrete Werte in einer Tabelle vorgegeben), verlangt die Suche nach einem kostenoptimalen Vektor ($\overrightarrow{p_{costoptimal}}$) den Einsatz von Methoden der Optimierung wie z.B. lineare oder mehrdimensionale Optimierung, Evolutionäre Algorithmen o.a. [Michalewicz und Fogel 2000].
Wenn ein akzeptierbarer Vektor nicht gefunden werden kannn, dann ist es notwendig ein oder mehrere angenommene Parameter der indirekt risikobeeinflussenden Ressourcen zu ändern. Nach erneuter Ermittlung der Risikocharakteristiken R_i kann anschließend mit der Suche fortgefahren werden.
Da es generell nicht immer möglich ist, eine Beschreibung in Form einer mathematischen Gleichung zwischen allen Verlässlichkeitsparametern und dem resultierenden

betrieblichen Risiko herauszufinden, kann die Suche nach einem risikooptimalen Vektor $\overrightarrow{p_{riskoptimal}}$ schon eine komplexe Optimierungsaufgabe darstellen. Das *PROFUND*-Modell bleibt dabei die einzige Beschreibung der Beziehung der Verlässlichkeitsparameter zum Risiko. Deswegen ist für die Suche nach einem kostenoptimalen Vektor $\overrightarrow{p_{costoptimal}}$ sehr vorteilhaft, wenn die Kostenfunktionen einzelner funktionalen Ressourcen direkt in die Petrinetzmodellierung integriert werden können. Ein praktisch anwendbarer Ansatz solcher Integration kann in [Trost et al. 2005] [Pozsgai und Bertsche 2005] gefunden werden.

Sensitivitätsanalyse des Beispieles aus der Streckensicherung Abbildung 6.12 zeigt die Ergebnisse der Sensitivitätsanalyse des Beispielmodells aus der Streckensicherung. Es handelt sich dabei um die Untersuchung des Risikoeinflusses der vier betrachteten gefährlichen Ausfälle der streckenseitigen Fahrwegsicherung (ortsbezogene Ausfälle *TRC1-ItH-time*, *TRC2-ItH-time*, *TRC3-ItH-time*) und Gesamtausfall (*TRC123-ItH-time* - Abb. 5.24) sowie auch des möglichen Ausfalls der zugseitigen Fahrzeugsicherung (*Enters-Train-with-failed-ATP*, s. auch Abb. 5.25 und Unterkap. 5.4.2). Die Risikowerte individueller funktionalen Ressourcen wurden bei unterdrücktem Einfluss der Ausfälle aller anderen Ressource ermitteltn. Abbildung zeigt auch die extrapolierte Funktionen der Näherungsverläufe mit entsprechenden Korrelationsfaktoren K^2. Während bei den ortsbezogenen Ausfällen eine externe Ausfalloffenbarung nur durch eine Gefahrsituation in dem Betriebsprozess angenommen wurde (*TRC1-HeFS*), wurde bei dem Gesamtausfall der streckenseitigen Sicherung mit einer Hazardoffenbarungszeit von einer halben Stunde gerechnet (*TRC123-HeFS-time*).
Als Verlässlichkeitsparameter der betrachteten sicherheitsrelevanten funktionalen Ressourcen wurden die Raten der gefährlichen Ausfälle nach der Exponentialverteilung angenommen. Die Ergebnisse der Simulation und darauf basierter Extrapolation zeigen, dass den größten Risikobeitrag die möglichen ortsbezogenen Hazardzustände (Hazardrate der *TRC1, TRC2, TRC3*) der Streckensicherung bringen, deren Offenbarung und Überführung in einen sicheren Fehlzustand erst durch eine Gefahrsituation in dem Eisenbahnbetrieb vorgesehen ist. Dagegen äußert sich der zeitbegrenzte Totalausfall der Streckensicherung (mittlere Zeit von 30 min) durch ein etwa 10-fach kleineres betriebliches Risiko.
Im Gegensatz zu den Ausfällen der direkt risikobeeinflussenden Fahrwegsicherung sind die negativen Folgen eines Ausfalles der Fahrzeugsicherung nur bei gleichzeitigem Versagen des Menschen relevant (Vorbeifahrt des Lokführers an einem haltzeigenden Signal). Um das Risikopotential auswerten zu können, müsste die Verlässlichkeit des menschlichen Verhaltens daher vorab konstant angenommen werden (hier beträgt die angenommene Wahrscheinlichkeit des Fehlverhaltens des Lokführers 10 Prozent).
Die in Abbildung 6.12 dargestellte Charakteristik des Risikobeitrages des gefährlichen

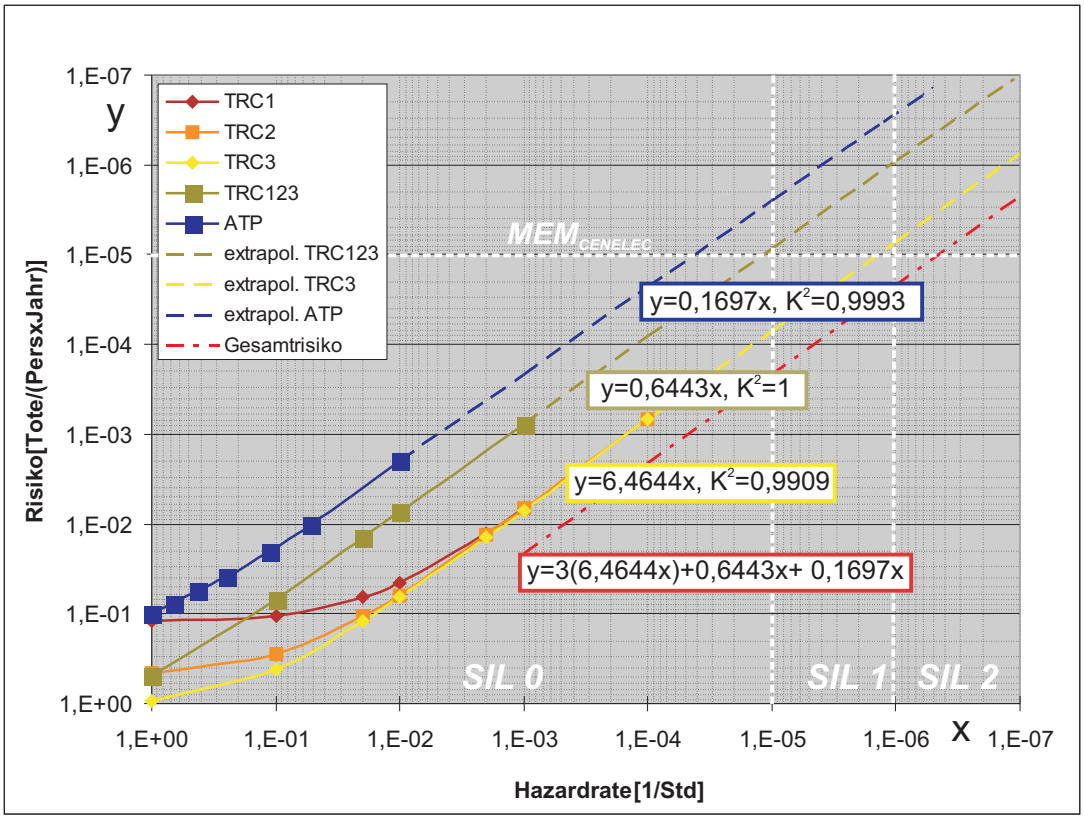

Abbildung 6.12: Risikoeinflüsse der betrachteten gefährlichen Ausfälle in dem Beispielmodell der Streckensicherung mit zugehörigen Näherungsverläufen und Korrelationsfaktoren

Ausfalls der Fahrzeugsicherung (ATP) integriert die angenommene Verlässlichkeit des menschlichen Verhaltens. Dadurch ist die Bedingung der Unabhängigkeit der risikobeitragenden Verlässlichkeitsparameter erfüllt und das Gesamtrisiko als Summe einzelner Risikobeiträge kann ausgewertet werden:

$$R_{Line} = R_{TRC1} + R_{TRC2} + R_{TRC3} + R_{TRC123} + R_{ATP} \tag{6.12}$$

Anhand der durchgeführten Extrapolationen der Näherungsfunktionen konnte die folgende mathematische Abhängigkeit abgeleitet werden:

$$R_{Line} = 3(6,4644 \cdot Hr_{TRC1}) + 0,6443 \cdot Hr_{TRC123} + 0,1697 \cdot Hr_{ATP} \mid P_{DriverSPAD} = 0,1 \tag{6.13}$$

wobei die Hazardraten der einzelnen funktionalen Ressourcen $Hr_{TRC1} = Hr_{TRC2} = Hr_{TRC3}$, Hr_{TRC123}, Hr_{ATP} und der angenommene Parameter $P_{DriverSPAD}$ den Vektor der Verlässlichkeitsparameter $\overrightarrow{p}$ bilden.
Die rot gezeichnete Charakteristik zeigt den möglichen Verlauf unter Annahme von gleich großen Verlässlichkeitsparametern aller betrachteten gefährlichen Ausfälle.
Wie durch die qualitative Analayse des funktionalen Modells bestätigt werden konnte, weist die betrachtete Systemfunktionalität kein Restrisiko R_F aus (s. Unterkap. 6.2.2). Diese Tatsache bestätigen auch die ermittelten Risikocharakteristiken.
Eine andere Darstellung bietet Abbildung 6.13, die die Abhängigkeit des Gesamtrisikos von der Größe der Verlässlichkeitsparameter der Fahrweg- und Fahrzeugsicherung zeigt (angenommenes Verhältnis zwischen dem Totalausfall und ortsbezogenen Ausfällen der Fahrwegsicherung war 1:3).
Die durch Simulation erhaltenen Charakteristiken des Risikoeinflusses der betrachteten Ausfälle der Fahrweg- und Fahrzeugsicherung wurden durch mathematische Funktionen approximiert und extrapoliert. Anhand der herausgefundenen funktionalen Abhängigkeiten einzelner gefährlicher Ausfälle konnte die allgemeine Gleichung für das Gesamtrisiko der Ausfälle der direkt risikobeeinflussenden Ressourcen bestimmt werden (s. Abb. 6.12). Diese Gleichung kann durch Optimierung zur Ableitung der quantitativen funktionalen Sicherheitsanforderungen angewendet werden.

6.2.4 Die funktionalen Sicherheitsanforderungen

Zulässige Ausfallraten

Die Ableitung der quantitativen funktionalen Sicherheitsanforderungen basiert auf der Optimierung. Da die hohen Sicherheitsanforderungen mit kostenintensiven technischen Lösungen verbunden sind, ist das Ziel dieser Optimierung, die notwendige Risikoreduktion durch möglichst niedrige Sicherheitsanforderungen zu erfüllen. Die quantitativen

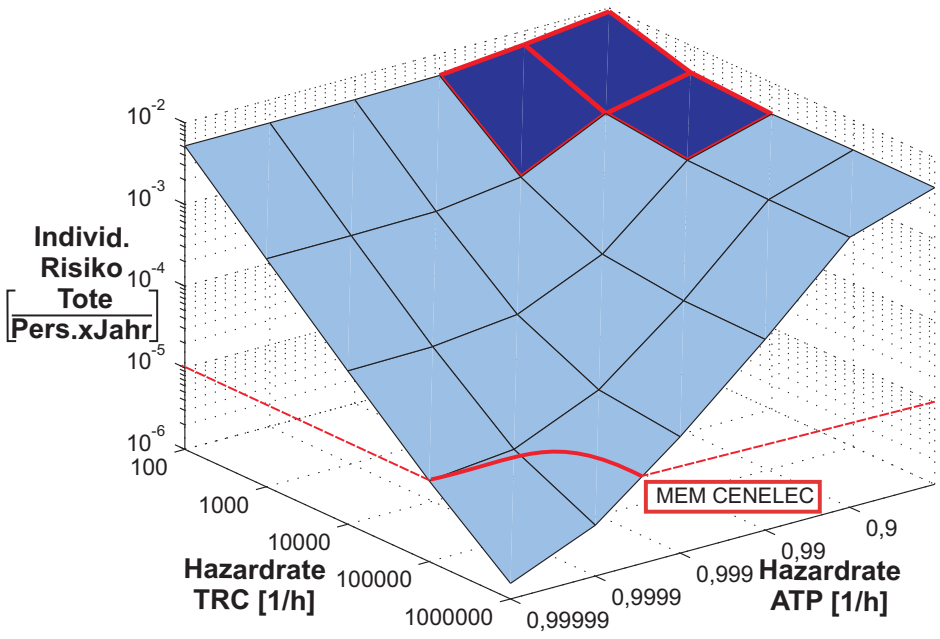

Abbildung 6.13: Abhängigkeit des betrieblichen Risikos von den Verlässlichkeitsparametern der Fahrwegsicherung TRC und Fahrzeugsicherung ATP des Beispieles aus der Streckensicherung

Sicherheitsanforderungen können durch die zulässigen Raten gefährlicher funktionaler Ausfälle oder durch die Sicherheitsanforderungsstufen (SIL - Safety Integrity Levels, s. Kap.2) definiert werden.

Angenommene Offenbarungsmechanismen

Neben der Angabe von zulässigen Ausfallraten der Funktionen ist es notwendig, auch die angenommenen Offenbarungsmechnismen anzugeben bzw. für unterschiedliche Hazardverlaufsarten entsprechende zulässige Ausfallraten der sicherheitsrelevanten Funktionen zu definieren. Dieser Fall tritt dann auf, wenn die Offenbarung der funktionalen Hazardzustände von externen eisenbahnprozessspezifischen Parametern (z.B. Dichte des Verkehrs, Instandhaltung benachbahrter Systeme usw.) abhängt. Hier besteht die Aufgabe, eine Ersatztransition zu finden (s. auch Unterkap. 5.5.2), deren temporale Parameter diese Wirkung des Eisenbahnbetriebsprozesses geeignet abbildet.
Eine Möglichkeit bietet die Annahme, dass der gesuchte Einfluss des Eisenbahnbetriebsprozesses den Charakter einer Exponentialverteilung hat. Durch eine Analyse des Modells wird nach so einer Rate der Hazarderkennung gesucht, die den gleichen Risikobeitrag der funktionalen Ressource im Betriebsprozess bewirkt. Da die breite Streuung des Temporalparameters einer Exponentialverteilung (beinhaltet auch sehr lange Hazarderkennngszeiten) nur ihre Verwendung als Ersatzverteilung erlaubt, ist für eine genaue (sichere) Bestimmung der Ersatztransition eine Analyse des tatsächlichen stochastischen Charakters des Einflusses oft notwendig. Möglichkeiten dazu bietet die transiente analytisch- oder simulationsbasierte Analyse, die den lebenszeitabhängigen Verlauf der Temporalcharakteristik des externen Einflusses ermittelt. Neben der Exponentialverteilung können dabei auch andere Verteilungen verwendet werden, bzw. es kann eine *konservative Exponentialverteilung* angenommen werden, die den schlimmsten Fall der tatsächlichen Verteilung der Hazardzustandserkennung abdeckt.
Neben der Angabe der Parameter der Offenbarungsmechanismen durch die Rate der Erkennung des Hazardzustandes (nachdem dieser aufgetreten ist) ist es möglich, auch die maximale zulässige Hazardauftrittswahrscheinlichkeit mit entsprechender Temporalcharakteristik zu verwenden.

Funktionale Sicherheitsanforderungen des Beispieles aus der Streckensicherung Abbildung 6.14 zeigt die mögliche Aufteilung der quantitativen Sicherheitsanforderungen zwischen strecken- und zugseitiger Funktionalität der Zugfolgesicherung aus dem behandelten Beispiel unter Annahme der betrachteten Hazardverlaufsarten (externen Hazardoffenbarungsmechanismen).
In diesem konkreten Fall ist es offensichtlich, dass eine optimale Aufteilung im Bereich von oberen Grenzen von SIL 0 für die zugseitige und von SIL 2 für die streckenseitige

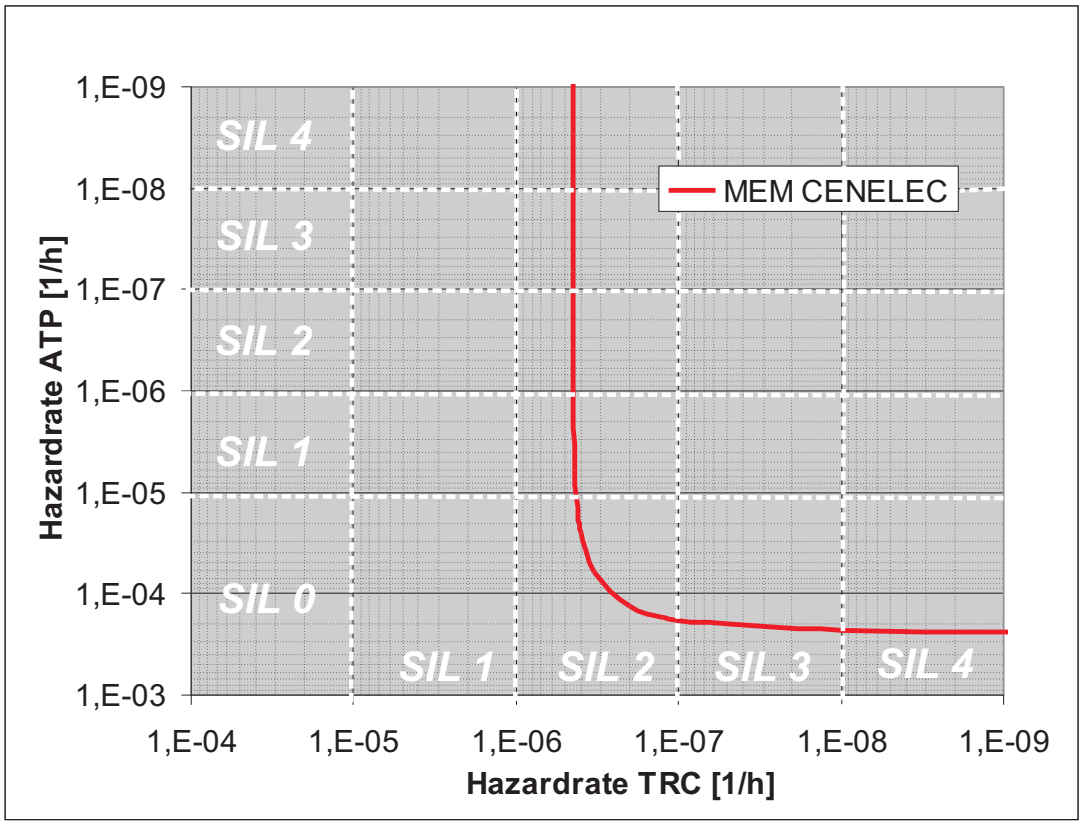

Abbildung 6.14: Quantitative funktionale Sicherheitsanforderungen für die Fahrweg- (TRC) und Fahrzeugsicherung (ATP) des betrachteten Beispiels

Funktionalität liegen würde. Über die genauen Werte der zulässigen Raten der gefährlichen Ausfälle könnte anhand der bekannten Kostenfunktionen entschieden werden. Die Definition der quantitativen Sicherheitsanforderungen für jede sicherheitsrelevante funktionale Ressource schließt die Aufgabe der Risikoanalyse des Eisenbahnbetriebes ab.

6.3 Gefährdungsanalyse der Systemimplementierung

Die grundsätzliche Aufgabe der Gefährdungsanalyse ist, anhand des Modells der Systemimplementierung diejenigen Parameter des Verlässlichkeitsverhaltens der Implementierungsressourcen herauszufinden, die die Erfüllung der durch die Risikoanalyse des Eisenbahnbetriebes gesetzten quantitativen funktionalen Sicherheitsanforderungen garantieren.
Die Gefährdungsanalyse steht oft in enger Beziehung mit dem Prozess der Modellierung der Systemimplementierung. Meistens entscheiden nämlich gerade die Ergebnisse der Gefährdungsanalyse über weitere Modellierungsverfeinerung oder -erweiterung. Ein typisches Beispiel dafür ist die Erweiterung des Modells um eine Diagnoseeinheit oder Redundanzfunktion, deren Ziel es ist, die Implementierung von höheren funktionalen Sicherheitsanforderungen mit Komponenten niedriger Sicherheitsanforderungsstufen zu realisieren.
Beim Erfüllen der funktionalen Sicherheitsanforderungen ist es einerseits notwendig zu prüfen, dass sich die Auftrittsrate des globalen gefährlichen Zustandes der Implementierung während der gesamten vorgesehenen Betriebsdauer des Systems unterhalb der zulässigen Rate des gefährlichen funktionalen Ausfalles befindet. Anderseits ist nachzuweisen, dass die zugehörige maximale Ausfalloffenbarungszeit während der Betriebsdauer nicht überschritten wird, bzw. dass die Ausfallauftrittswahrscheinlichkeit auch noch durch die Implementierung unter dem zulässigen Wert bleibt.
Solange es die Modellkomplexität erlaubt, besteht auch die Möglichkeit das Modell der Systemimplementierung direkt mit dem Modell des Betriebsprozesses zu koppeln und die tatsächlich erreichte Risikoreduktion zu überprüfen. Durch diese Vorgehensweise kann manchmal eine bessere Auslegung der Sicherheitsziele für die einzelnen Systemkomponenten erreicht werden. Ein Beispiel eines solchen Vorgehens wird im Unterkapitel 7.6 gezeigt.

6.3.1 Analyse des Modells der Systemimplementierung

Auch für die Modellierung der Systemimplementierung können die beschriebenen Methoden der Modellverifikation und -validation angewendet werden. Neben dem Syntaxcheck und interaktiven Markenspiel können die Algorithmen der Bildung des Graphen

der globalen sicherheitsrelevanten Zustandsmengen und des Unfallbaumes genutzt werden.
In den Modellen der Systemimplementierung besteht meistens nicht mehr ein direkter Bezug zum Eisenbahnbetriebsprozess und zur Systemfunktionalität, sondern es handelt sich lediglich um die Verfeinerung der funktionalen Verlässlichkeitsmodelle. Dieses hat zur Folge, dass anstatt des bisher im Rahmen der Risikoanalyse zu Grunde gelegten unerwünschten betrieblichen Ereignisses (Unfalls) bei der Gefährdungsanalyse der Systemimplementierung der Auftritt der funktionalen Gefährdung zu untersuchen ist. Neben der stationären numerischen Analyse und Simulation können hier die transienten Analyseverfahren zum Nachweis der Erfüllung der gesetzten funktionalen Sicherheitsanforderungen angewendet werden.

6.3.2 Sicherheitsanforderungen der Systemimplementierung

Die Sicherheitsanforderungen der Systemimplementierung sind in Form von tolerierbaren Ausfallraten für vorgesehene Systemkomponenten zu definieren. Ebenso wie bei der Definition der funktionalen Sicherheitsanforderungen sind die Mechanismen der Offenbarung eines gefährlichen Komponentenfehlers anzugeben. Diese können in Form von Diagnoseintervallen oder Wartungsperioden festgelegt werden.

Implementierung mit Diagnose Abbildung 6.15 zeig die Analyseergebnisse eines Implementierungsmodells einer oder mehrerer technischer Komponenten in Verbindung mit einer Diagnoseeinheit, die in der Lage ist, innerhalb von einem Diagnoseintervall den gefährlichen Komponentenfehler zu erkennen und in einen sicheren (*fal-safe*) Zustand herbeizuführen. Ein konkretes Anwendungsbeispiel bietet dafür die Implementierung der ortsbezogenen Funktionalität der Fahrwegsicherung durch einen Gleisstromkreis, ein Signal und eine Diagnoseeinheit (s. Abb 5.30).
Die im Graphen gemachten Angaben der tolerierbaren Gefährdungsraten (THR - Tolerable Hazard Rates) stellen zwei mögliche Vorgaben der technischen Sicherheitsanforderungen mit dem Ziel dar, die funktionalen Sicherheitsanforderungen von SIL 2 zu erfüllen. Die Ergebnisse zeigen, dass die niedrigeren Sicherheitseigenschaften der technischen Komponente (z.B. von SIL 0) durch eine bessere Diagnose (hier von SIL 2) kompensiert werden können und dass auch höhere funktionale Sicherheitsanforderungen durch geeignete Überwachung von in Bezug auf Sicherheit schwächeren Implementierungskomponenten (hier ist die SIL-Differenz = 2) erreicht werden können. Über die endgültige Auslegung der Sicherheitsanforderungen an die einzelnen technischen Komponenten kann nach der Berücksichtigung von Herstellungs- und Betriebskosten entschieden werden. Im Graphen der Abbildung 6.15 sind auch die Anforderungen an

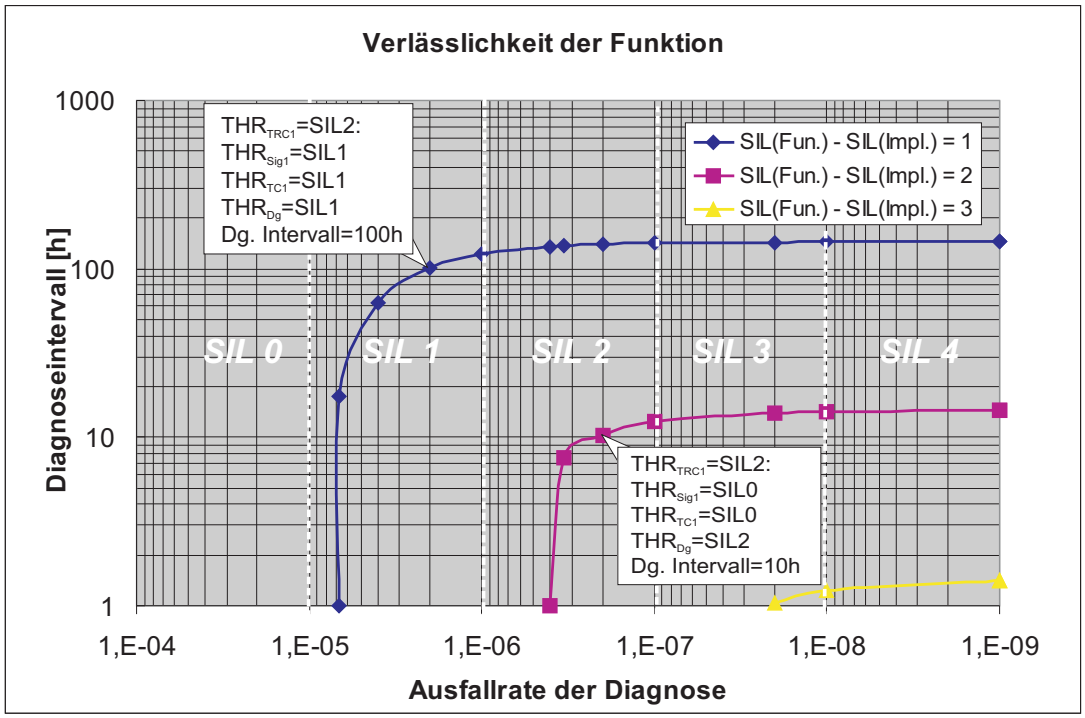

Abbildung 6.15: Sicherheitsanforderungen an die Implementierung der Fahrwegsicherung - TRC1

die Diagnostik von technischen Komponenten mit weiteren möglichen SIL-Differenzen zwischen der Funktionalität und ihrer Implementierung dargestellt.

Implementierung mit Redundanz Abbildung 6.16 zeigt die mögliche Verteilung der technischen Sicherheitsanforderungen der Implementierung in Form von THR's einer 2v3 Architektur mit einem Voter (s. Abb. 5.31). Wie ersichtlich ist, sind für die gegebenen funktionalen Sicherheitsanforderungen (z.B. SIL 2) die Sicherheitseigenschaften des Voters entscheidend. Diese können verringert werden nur unter Voraussetzung, dass die Sicherheitseigenschaften einzelner Kanäle mindestens die geforderten funktionalen Sicherheitsanforderungen erfüllen.

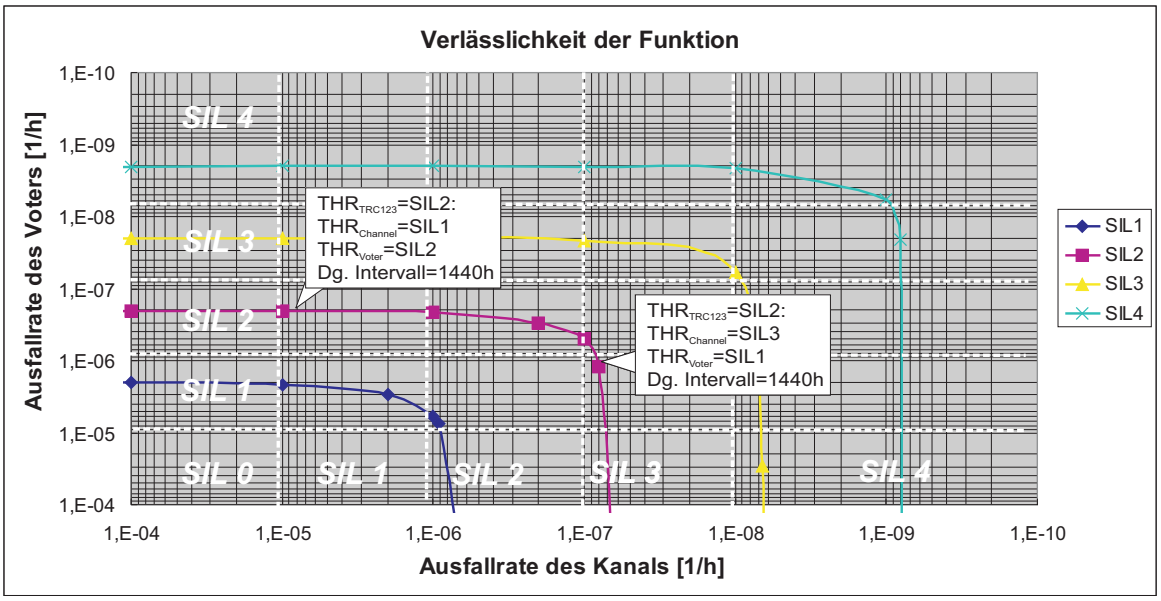

Abbildung 6.16: Sicherheitsanforderungen an die Implementierung der Fahrwegsicherung - TRC123

Auch bei dieser mehrkanaligen Architektur spielt die Offenbarungszeit des gefährlichen Komponentenfehlers eine bedeutende Rolle. In diesem Fall wurde eine entsprechende Diagnostik im Rahmen einer periodischen Wartung im Zeitabstand von 2 Monaten (1440 Stunden) angenommen. Die dargestellten Analyseergebnisse können zur Definition der technischen Sicherheitsanforderungen der Auswertungslogik des behandelten Beispiels der Fahrwegsicherung (Abb. 5.31) auf einer Strecke verwendet werden.

6.4 Zusammenfassung

Die Aufgabe der *PROFUND*-Analyse ist es, im ersten Schritt den Anwender bei der Modellbildung und Modellüberprüfung durch genannte Methoden der Modellverifikation und -validation zu unterstützen. Nur ein überprüftes Modell kann zur Risiko- bzw. Gefährdungsanalyse und zur Definition der quantitativen funktionalen bzw. technischen Sicherheitsanforderungen verwendet werden. Die modellbasierte Vorgehensweise ermöglicht, die gesuchten Sicherheitsziele optimal im Bezug auf das ermittelte Risiko im Eisenbahnbetriebsprozess und auf die Implementierungs- und Betriebskosten im Sinne des vorgegebenen akzeptierbaren Risikos auszulegen.

Kapitel 7

PROFUND-Anwendung am Beispiel Bahnübergang

Ziel dieses Kapitels ist es anhand eines weiteren praktischen Beispieles die Anwendung der in dieser Arbeit vorgestellten *PROFUND*-Methode kompakt darzustellen. Als Anwendungsbeispiel wurde hier der Bahnübergang gewählt, der eine niveaugleiche Kreuzung zwischen dem Eisenbahn- und dem Straßenverkehr darstellt. Diese Wahl basiert auf den folgenden beiden Gründen:

- Der Bahnübergang ist ein wichtiges Objekt der Sicherheitsanalyse. Jedes Jahr werden an Bahnübergängen Europas bei ca. 1200 Unfällen mehr als 330 Menschen getötet [EuroStat 2006]. Die Bahnübergänge bedeuten nicht nur eine Schwachstelle des Straßenverkehrs sondern eine höchst signifikante Unfallquelle des Eisenbahnverkehrs. Bei vielen Eisenbahnen in der Welt repräsentieren die Bahnübergangsunfälle bis zu 50% aller Todesfälle in deren Betrieb.

- Der Bahnübergang ist ein geeignetes Beispiel zum Testen formaler Methoden [Hänsel et al.]: Der Verkehrsbetrieb an einem Bahnübergang sowie die Funktionalität eines Bahnübergangssicherungssystems beinhalten viele typische Verhaltens- und Strukturaspekte eines Eisenbahnleit- und -sicherungssystems. Außerdem kann ein Bahnübergang, meistens ohne viele Schnittstellen zu Nachbarsystemen, als ein selbstständiges System betrachtet werden, was sich bei der Modellierung durch eine beherrschbare und überschaubare Komplexität auszeichnet.

7.1 Gefahrenanalyse eines Bahnübergangs

Wie im Unterkapitel 5.2 erwähnt wurde, beinhaltet eine Gefahrenanalyse die Identifikation der relevanten Systemfunktionen und der sich im Betrieb ergebenden Gefahren.

7.1.1 Systemdefinition

Das als Beispiel genommene System Bahnübergang besteht aus den sich kreuzenden Verkehrswegen des Eisenbahn- und Straßenverkehrs. Abbildung 7.1 zeigt die einfachste Version einer solchen Kreuzung, einen ungesicherten Bahnübergang. Ein sicherer Betrieb hängt in diesem Falle nur vom korrekten Verhalten der Nutzer des Straßenverkehrs, der KFZ-Fahrer, ab. Zur Ausrüstung gehören die entsprechenden Verkehrszeichen (Andreaskreuze und deren Ankündigungen), die den KFZ-Fahrer über die Vorfahrt der Eisenbahnfahrzeuge informieren. Von der Seite des Eisenbahnverkehrs liegt meistens nur die Verpflichtung einer akustischen Warnung vor, die der Lokführer in angegebener Entfernung vor dem Bahnübergang ausgeben soll. Da der KFZ-Fahrer auf den kommenden Zug nur im Rahmen seines Sichtbereiches reagieren kann, stellt diese Sichtbeschränkung die Systemgrenze auf der Seite des Straßenverkehrs dar (Annäherungsbereich). Auf ähnliche Weise könnte man die Systemgrenze eines ungesicherten Bahnübergangs auf der Eisenbahnstrecke definieren, aber eine entsprechende Änderung des Fahrverhaltens des Zuges ist meistens ausgeschlossen.

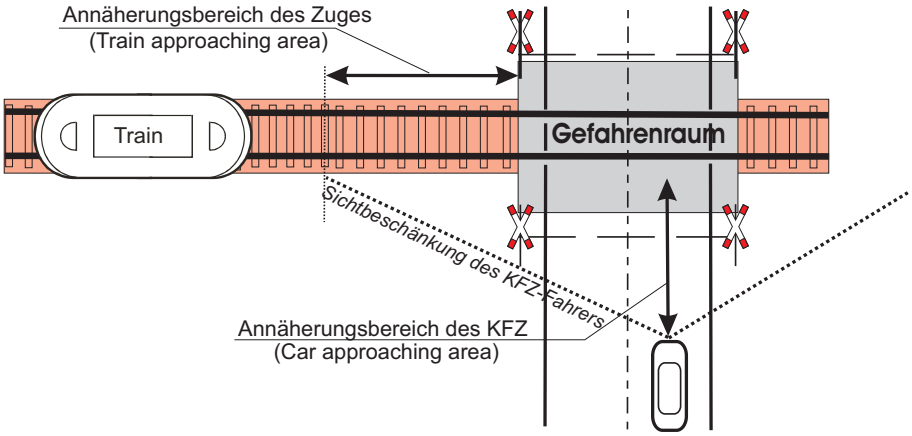

Abbildung 7.1: Verkehrsbedingungen an einem ungesicherten Bahnübergang

Bei Verkehrswegen mit höheren Verkehrsflüssen muss die Sicherheit auf dem Bahnübergang mit einem Bahnübergangssicherungssystem gewährt werden. Seine Aufgabe ist es, die Benutzer des Straßenverkehrs vor dem sich nähernden Eisenbahnfahrzeug rechtzeitig zu warnen. Im Allgemeinen können die folgenden fünf grundsätzlichen Funktionen eines Bahnübergangssicherungssystems identifiziert werden:

- Zugerkennung, die die Anwesenheit eines Eisenbahnfahrzeuges in einem ausreichenden Abstand vor dem Bahnübergang erkennt. Die Entfernung des Aktivierungsbereiches ist von maximaler Streckengeschwindigkeit und der Sicherungsart des Bahnübergangs abhängig,

- Aktivierung des Bahnübergangssicherungssystems anhand der Information der Zugerkennung,
- Warnungsanzeige für die Teilnehmer des Straßenverkehrs,
- Erkennung der Räumung des Gefahrenbereiches des Bahnübergangs, die das Verlassen des letzen Eisenbahnfahrzeuges detektiert,
- Deaktivierung des Bahnübergangssicherungssystems anhand der Information der Erkennung der Räumung des Gefahrenbereichs.

Abbildung 7.2 zeigt die möglichen Ressourcen der technische Implementierung eines solchen gesicherten Bahnübergangs, wobei hier zur Warnung der Nutzer des Straßenverkehrs ein Lichtzeichen verwendet wurde.

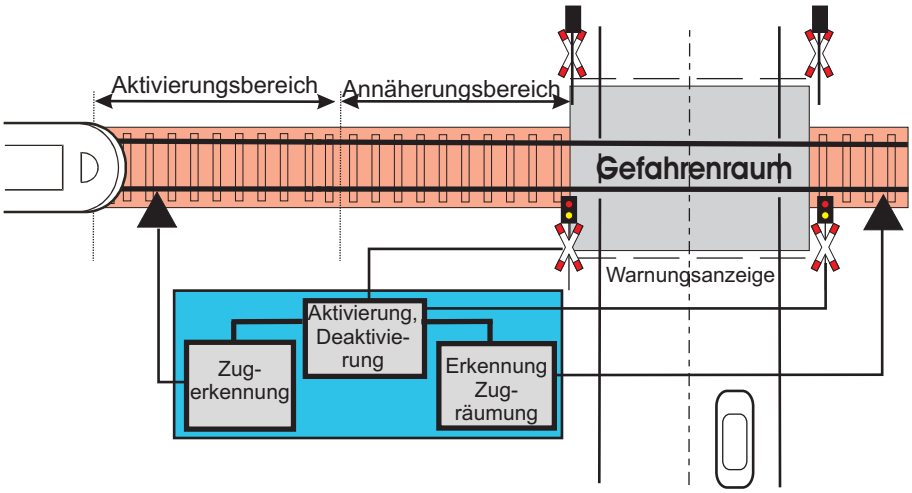

Abbildung 7.2: Eine Implementierung der grundsätzlichen Funktionalität eines gesicherten Bahnübergangs

Im Falle des technisch gesicherten Bahnübergangs wird die Systemgrenze auf Seiten des Schienenverkehrs durch den Anfang des Aktivierungsbereiches der Zugerkennung gegeben.
Das hier behandelte Beispiel betrachtet keine Funktion eines Überwachungssignals, welches den Lokführer über ein mögliches Versagen des Sicherungsvorganges informieren könnte. Dagegen wird angenommen, dass eine Überwachung der korrekten Sicherungsfunktion über eine Verbindung mit dem Arbeitsplatz des Fahrdienstleiters in der nächsten Betriebstelle erfolgt.

7.1.2 Gefahrenidentifikation

Eine generelle gefährliche Situation am Bahnübergang stellt die gleichzeitige Belegung des Gefahrenraums (Danger Zone) durch ein Straßen- und ein Eisenbahnfahrzeug dar. Diese Situation führt in den meisten Fällen zur unmittelbaren Kollision (Zusammenprall), die in einem ungünstigen Fall auch zu einer Entgleisung des Zuges führen kann. Tabelle 7.1 stellt in Form einer FMEA (Failure Modes Effect Analysis) Tabelle die potenziellen Folgen des Versagens einzelner identifizierter Funktionen des Bahnübergangsicherung.

Funktion	Ausfallart	Auswirkung	Gefährdung
Zugerkennung im Aktivierungsbereich	Verspätete oder keine Erkennung des Zuges	Verspätete oder keine Sicherung des BÜ	Ja
Aktivierung	Verspätete oder keine Aktivierung	Verspätete oder keine Aktivierung des BÜ	Ja
Warnungsanzeige	Verspätete, unausreichende oder keine Warnunganzeige	Unausreichende Warnung des Straßenverkehrs	Ja, insbesondere bei gleichzeitigem Ausbleiben aller Warnungsarten
Erkennung der Räumung	Verspätete oder keine Erkennung der BÜ-Räumung	Verspätete oder keine Entsicherung des BÜ	Möglich bei längerer Schließzeiten durch Mißachtung der Warnung
Deaktivierung	Verspätete oder keine Deaktivierung	Verspätete oder keine Deaktivierung des BÜ	Möglich bei längerer Schließzeiten durch Mißachtung der Warnung

Tabelle 7.1: FMEA Tabelle der Funktionen der Bahnübergangsicherung

Abbildung 7.3 zeigt in Form eines Ereignisbaums möglichen Folgen betrieblicher Ereignisse, die zu einem Unfall führen können. Dabei wurde das Regelverhalten grün, die gefährlichen Situationen gelb und die Unfälle rot markiert.

Wie ersichtlich ist, hat neben dem Versagen der Bahnübergangssicherungsanlage (BÜSA) das Fehlverhalten des KFZ-Fahrers ein großes Ursachenpotenzial zum Unfallauftritt. Der Störungsbaum in Abbildung 7.4 fasst die möglichen Ursachen der Kollision zwischen einem Zug und einem KFZ zusammen.

Eine weitere Gefahr ergibt sich durch eine mögliche Kollision des Straßenfahrzeuges mit der Bahnübergangsanlage im Falle einer unzeitigen Folge der Warnzeichen, z.B. Schließung einer Halbschranke vor der Anzeige des halt zeigenden Lichtzeichens oder durch einen Noteingriff des KFZ Fahrers mit dem Ziel, einen Zusammenstoß mit dem Zug zu vermeiden. Da die genauen Ursachen und Folgen dieser Gefahr den Rahmen und das Ziel dieses Kapitels sprengen würden, wird sie bei weiteren Betrachtungen außer Acht gelassen.

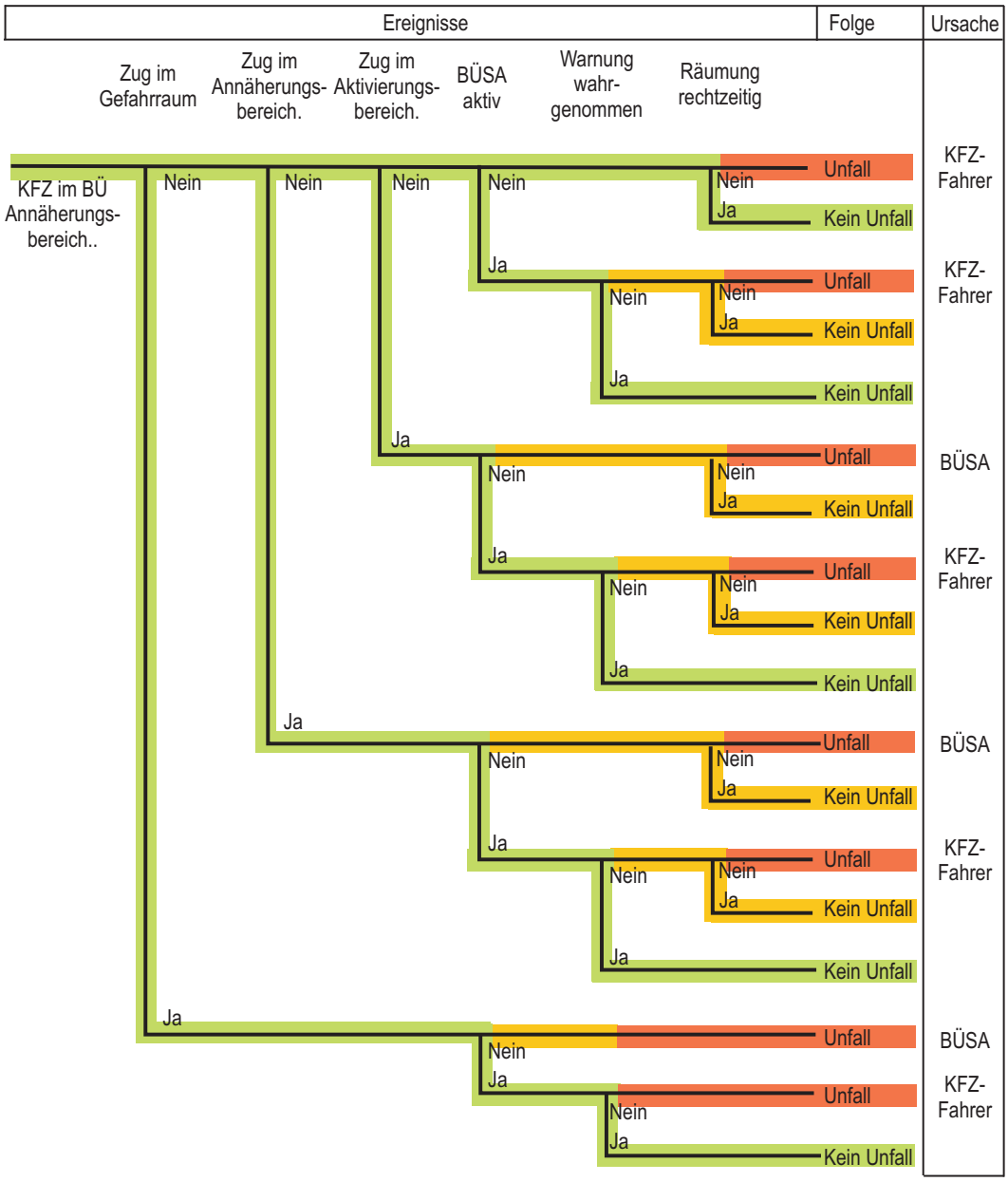

Abbildung 7.3: Ereignisbaum der Kollision auf einem technisch gesicherten Bahnübergang

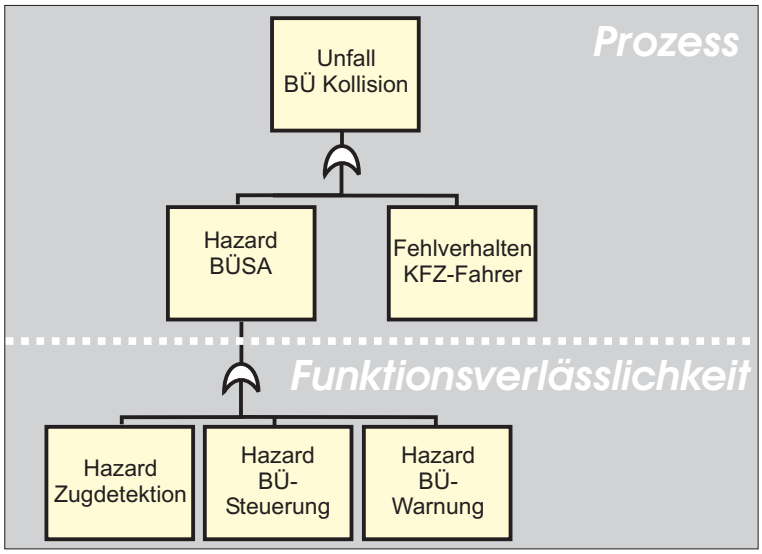

Abbildung 7.4: Unfallbaum der Kollision auf einem technisch gesicherten Bahnübergang

7.2 Beschreibung der BÜ-Unfallfolgen

Eine Voraussetzung zur Beschreibung aller möglichen Folgen der Unfälle am Bahnübergang ist die Identifikation der potentiellen Unfallsituationen. Dies beinhaltet eine Berücksichtigung unterschiedlicher KFZ-Typen, deren Geschwindigkeit bei der Annäherung sowie die unterschiedlichen Zugarten. Diese sind exemplarbezogen für jeden untersuchten Bahnübergang spezifisch, inklusive seiner örtlichen Bedingungen.

Zur Vereinfachung wird in diesem Kapitel als Beispiel nur eine repräsentative Unfallsituation am Bahnübergang betrachtet, die als Obermenge aller weiteren ähnlichen Unfälle gesehen werden kann. Abbildung 7.5 zeigt in der eingeführten Petrinetznotation (Unterkapitel 5.3.2) die Vorschrift zur Auswertung des individuellen Risikos eines KFZ-Fahrers bei Benutzung eines Bahnübergangs.

Neben den statistischen Werten, gekennzeichnet mit einer Marke, bilden den Eingang der dargestellten Berechnung die jährliche Anzahl der Kollisionen (Zusammenstöße) zwischen einem Zug und einem KFZ und die Angabe zur Dichte des Straßenverkehrsflusses in KFZ/Std des untersuchten Bahnüberganges. Bei den Berechnungen des individuellen Risikos wurden exemplarisch die mittleren statistischen Werte angenommen: 1,5 Personen pro KFZ; 500 Nutzungen eines KFZ-Fahrers pro Jahr; 0,3 relative Tote pro Bahnübergangsunfall [Braband und Lenartz 2000].

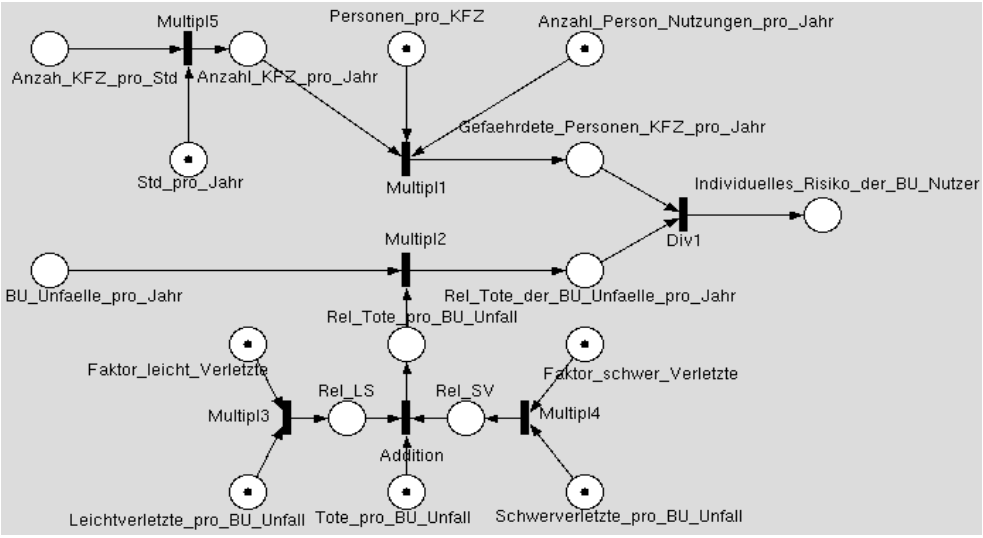

Abbildung 7.5: Berechnung des individuellen Risikos der KFZ-Nutzer eines Bahnüberganges

7.3 Bildung und Analyse des BÜ-Prozessmodells

7.3.1 Modellbildung

Um die Auswertung des betrieblichen Risikos an einem Bahnübergang zu ermöglichen, soll im Sinne der *PROFUND*-Methode ein geeignetes Modell der relevanten Verkehrsprozesse gebildet werden. Abbildung 7.6 zeigt die oberste Ebene des Prozessmodells, welches das Unfallpotential des Bahnüberganges darstellt. Neben der Kollision zwischen dem Straßen- und Eisenbahnfahrzeug wurde hier auch die Kollision mit der Bahnübergangsanlage ohne weitere Verfeinerung dargestellt.
Die Verfeinerung der Instanz *Hazard-Situations* in Abbildung 7.7 beinhaltet die eigentliche Beschreibung der beiden Verkehrsprozesse. In beiden Fällen wird die Bewegung des entsprechenden Fahrzeuges im jeweiligen Annäherungsbereich (*Car-approaching* bzw. *Train-approaching*), Gefahrraum (*Car-in-DZ* bzw. *Train-in-DZ*) und außerhalb des Bahnübergangsbereichs (*Car-out-of-LC* bzw. *Train-out-of-LC*) betrachtet. Die entsprechenden dazwischenstehenden Transitionen beschreiben die Bewegung der Fahrzeuge. Die Transitionen *Car-enters-approaching-area* und *Train-enters-approaching-area* sind parametrisiert mit stochastischer Verteilung, die den Folgezeiten zwischen zwei Straßen- bzw. Eisenbahnfahrzeugen entspricht. Als Beispiel wurde hier die Exponentialverteilung verwendet. Die Zeitparameter weiterer Transitionen (*Car-in-DZ* und *Train-in-DZ*) entsprechen der mittleren Verweildauer der Fahrzeuge in jeweiligen Bereichen, wobei diese ebenfalls mit einer Exponentialverteilung angenähert wurden. Für

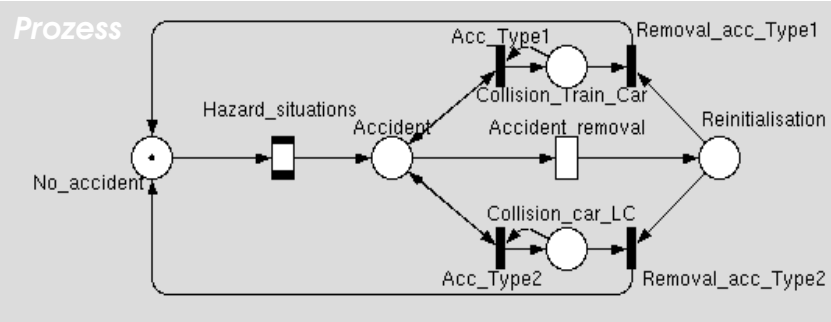

Abbildung 7.6: Modellierung der Unfallarten im Betriebsprozess auf einem Bahnübergang

die Verweilzeit des Zuges in dem Annäherungsbereich (*Train-enters-DZ*) wurde eine konstante Zeit (entsprechend der maximalen Streckengeschwindigkeit - *Worst Case*) angenommen. Die erhöhte Anzahl der Marken auf dem Platz *Car-out-of-LC* sorgt für die Nachbildung eines quasi-kontinuierlichen Straßenverkehrsflusses.

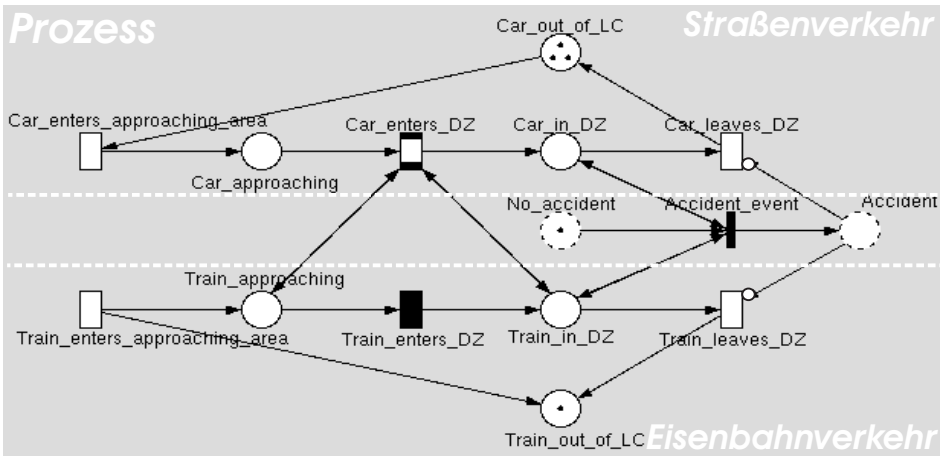

Abbildung 7.7: Modellierung des Betriebsprozesses auf dem Bahnübergang

Die Instanz *Car-enters-DZ* beschreibt das mögliche Verhalten der KFZ-Fahrer bei der Einfahrt in den Gefahrenbereich des hier betrachteten ungesicherten Bahnübergangs. Diese Verfeinerung ist in Abbildung 7.8 dargestellt.
Die Modellierung setzt voraus, dass es möglich ist, die KFZ-Fahrer nach ihrem Verhalten wie folgt zu unterscheiden:

- die Fahrer (I), die den Bahnübergang nie überqueren solange sich ein Zug im Annäherungsbereich befindet

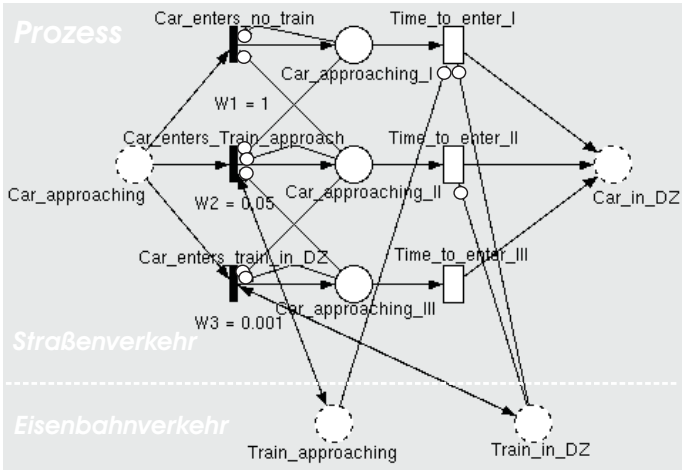

Abbildung 7.8: Beschreibung menschliches Verhaltens auf einem ungesicherten Bahnübergang

- die Fahrer (II), die aus eigenem Willen, wegen der verschlechterten Sichtverhältnisse oder fahrzeugbedingt, in den Gefahrenraum des Bahnübergangs trotz eines Zuges im Annäherungsbereich einfahren
- die Fahrer (III), die wegen der verschlechterten Sichtverhältnisse oder fahrzeugbedingt in den Gefahrenraum des Bahnübergangs trotz eines durchfahrenden Zuges einfahren.

Die proportionale Aufteilung dieser Fahrergruppen ist in der Modellierung durch Gewichtung der kausalen Transitionen *Car-enters-no-train*, *Car-enters-train-approaching*, *Car-enters-train-in-DZ* gegeben (*W1*, *W2*, *W3*). Die im Beispiel verwendete Quantifizierung dieser Gewichte (1/0,05/0,001) modelliert die Situation, dass ein KFZ in den Gefahrenbereich mit

- ca. 5% Wahrscheinlichkeit einfährt, wenn sich zugleich ein Zug im Annäherungsbereich befindet und
- mit etwa 0,1% Wahrscheinlichkeit einfährt, wenn ein Zug bereits den Gefahrenraum durchfährt.

Die eingegebenen Werte können anhand von Verkehrsbeobachtungen und Unfallstatistiken abgeschätzt werden. Sie sollen auf jeden Fall im Bereich der *Worst-Case* Schätzungen liegen.
Das Zielverhalten ist durch die entsprechenden Abfragekanten und Inhibitoren zwischen dem Modell des Straßen- und Eisenbahnverkehrs beschrieben worden. Die Inhibitoren

von den Plätzen *Car-approaching-I* bis *III* sorgen für die Nachbildung der Warteschlange der Straßenfahrzeuge, in der das erste Fahrzeug vor dem Gefahrenraum die Einfahrt der anderen Fahrzeugen verhindert. Die Transitionen *Time-to-enter-I* bis *III* modellieren die entsprechende Verweildauer der Straßenfahrzeuge im Annäherungsbereich.
Das Verkehrsprozessmodell betrachtet direkt nur die unidirektionalen Verkehrsflüsse, seine bidirektionale Anwendung setzt die gleichen Verkehrsbedingungen (Geschwindigkeiten, Sichtbereiche usw.) voraus. Anderenfalls müsste eine Modellergänzung vorgenommen werden.

7.3.2 Analyse

Qualitative Analyse Neben dem Modellchecking und der interaktiven Simulation des Modellverhaltens bildet die Basis zur Verifikation und Validation der Graph von Mengen globaler sicherheitsrelevanter Zustände (s. Unterkapitel 6.2.1). Abbildung 7.9 zeigt einen solchen Graphen, der nach der Definition der relevanten Zustände aus dem Erreichbarkeitsgraphen des BÜ-Prozessmodells generiert werden konnte.

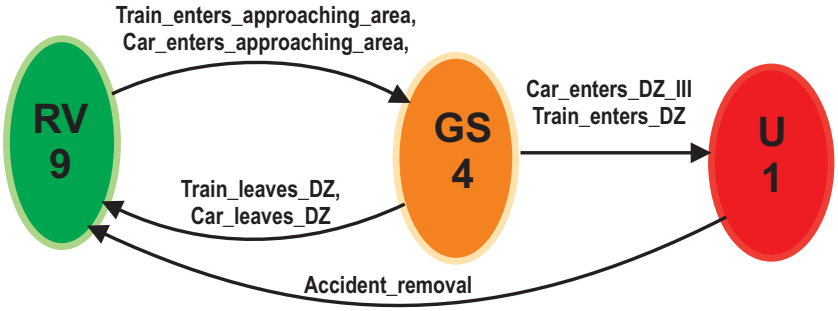

Abbildung 7.9: Graph von Mengen globaler sicherheitsrelevanter Zuständen des modellierten ungesicherten Bahnübergangs

Abbildung 7.10 zeigt den entsprechenden vollständigen Erreichbarkeitsgraphen mit farbig markierten relevanten Zuständen, der in diesem Falle aus überschaubaren 14 Knoten besteht.
Der einzige globale Unfallzustand ist durch die Markierung des Platzes *Accident* definiert. Als gefährlich sind alle globalen Zustände bezeichnet worden, aus denen ohne Möglichkeit menschlicher Verhinderung ein Unfall entstehen kann. Diese entsprechen den vier gefährlichen Situationen, in denen sich zu gleicher Zeit ein KFZ im Gefahrenraum und ein Zug in Annäherung befindet (markierte Plätze *Car-in-DZ* und *Train-approaching*), oder in denen sich mit einem Zug in Annäherungsbereichen auch ein KFZ im Annäherungsbereich befindet, ohne eine technisch oder menschlich bedingte Absicht, vor dem Gefahrenraum anzuhalten (markierte Plätze *Car-approaching-II*

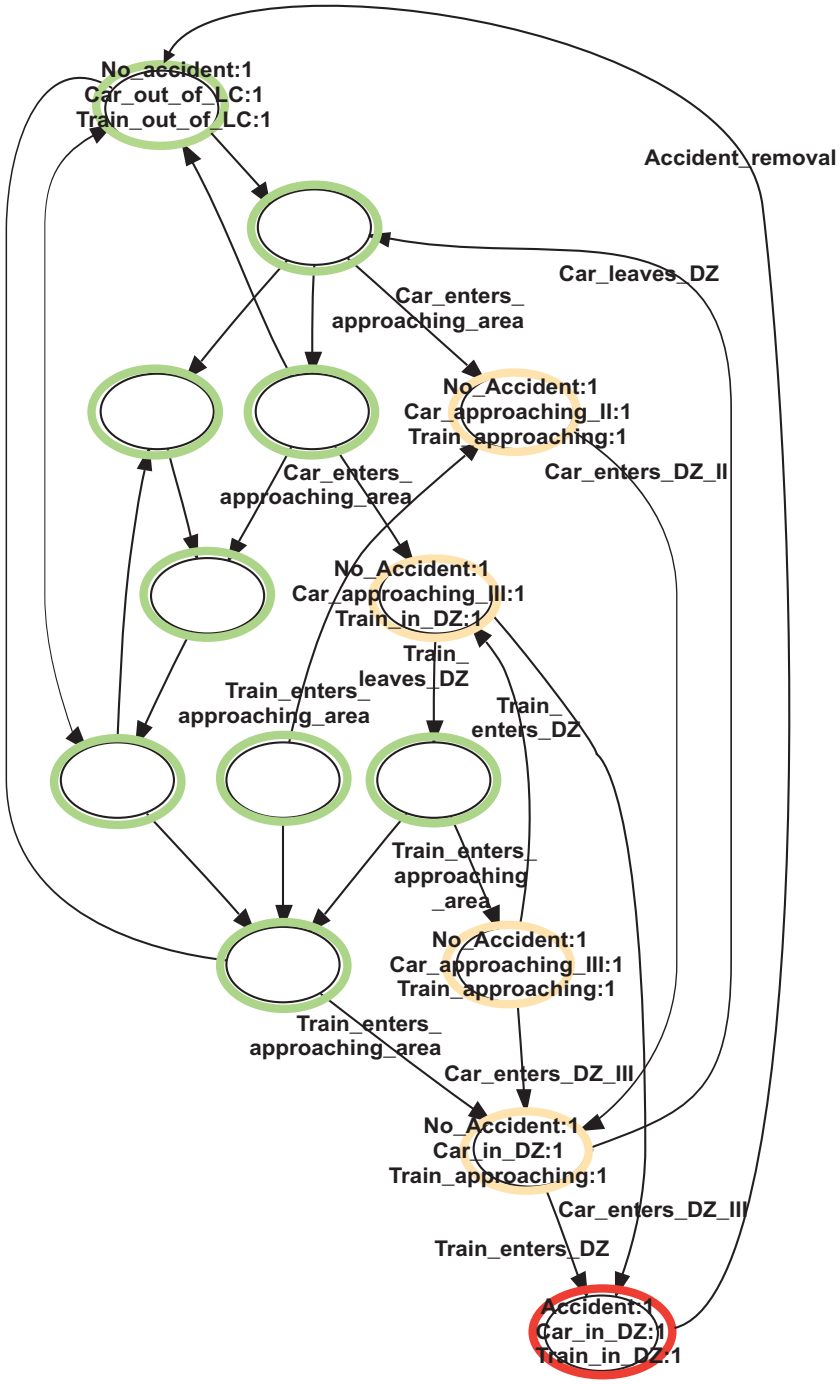

Abbildung 7.10: Erreichbarkeitsgraph des Modells des ungesicherten Bahnübergangs

und *Train-approaching*, oder *Car-approaching-III* und *Train-approaching* oder *Car-approaching-III* und *Train-in-DZ*). Alle restlichen Knoten des Erreichbarkeitsgraphen bilden das Regelverhalten des Prozessmodells.
Die bei der Generierung des Graphen von Mengen relevanter Zustände identifizierten, für den Mengenwechsel verantwortlichen Ereignisse können zur Modellvalidation mit dem im Rahmen der Gefahrenanalyse erstellten Ereignisbaum (Abbildung 7.3) verglichen werden. Mehrere Ereignisse eines Überganges repräsentieren dabei alternative Ursachen für einen Wechsel eines sicherheitsrelevanten Globalzustands.
Neben der Generierung des Graphen von Mengen globaler relevanter Zustände ist es möglich den Erreichbarkeitsgraph direkt qualitativ zu untersuchen. Einerseits kann man startend aus dem Unfallzustand durch eine Rückwärtsanalyse die Unfallursachen herausfinden, andererseits können bestimmte Sicherheitsanforderungen auf Gültigkeit überprüft werden. Die quantitativ basierte Definition der Sicherheit fordert jedoch, die qualitativen Aussagen mit quantitativen Auswertungen des resultierenden Risikos des Betriebes auf dem Bahnübergang zu ergänzen.

Quantitative Analyse Die wichtigste Aufgabe der quantitativen Analyse ist die Auswertung des Risikos. Zuvor empfiehlt es sich jedoch, bestimmte quantitative Auswertungen zur Validation des Modells durchzuführen. Im Falle des Bahnüberganges ist es möglich, aus den mittleren Zeiten zwischen den Fahrzeugen (Parameter des Modells) die entsprechenden Verkehrsflüsse des Straßen- und Eisenbahnverkehrs zu bestimmen. Das BÜ-Prozessmodell kann direkt zur Auswertung des kollektiven Risikos in Form der Unfallhäufigkeit/Jahr verwendet werden, dargestellt in Abbildung 7.11. Eine Multiplikation mit dem Fatalitätsfaktor eines Bahnübergangunfalles (0,3) [Braband und Lenartz 2000] ermöglicht das kollektive Risiko der am BÜ-Straßenverkehr teilnehmenden Personen in Toten/Jahr auszudrücken.
Die Auswertung des individuellen betrieblichen Risikos kann nach der Kopplung des BÜ-Prozessmodells mit dem Modell der Unfallfolgen (Abbildung 7.5) durchgeführt werden. Abbildung 7.12 zeigt die Abhängigkeit des individuellen Risikos der am Straßenverkehr teilnehmenden Personen von der Stärke der beteiligten Verkehrsflüsse.
Die resultierende Abhängigkeit bestätigt die Steigerung des individuellen Risikos mit steigender Dichte des Eisenbahnverkehrs. Auf der anderen Seite zeigt der Verlauf auch, dass das individuelle, sich aus der BÜ Nutzung ergebende Risiko einzelner im KFZ fahrender Personen beim Anstieg des Straßenverkehrflusses sinkt. Dies ist bedingt durch Bildung der Abhängigkeiten zwischen den hintereinander fahrenden KFZ, insbesondere Verhinderung einer unerlaubten Weiterfahrt eines KFZ durch ein anderes, vor dem Gefahrraum korrekt stehendes Fahrzeug. Die ermittelte Abhängigkeit bestätigt auch die Unfallstatistiken z.B. [Smith 2006] in denen die ungesicherten Bahnübergänge der

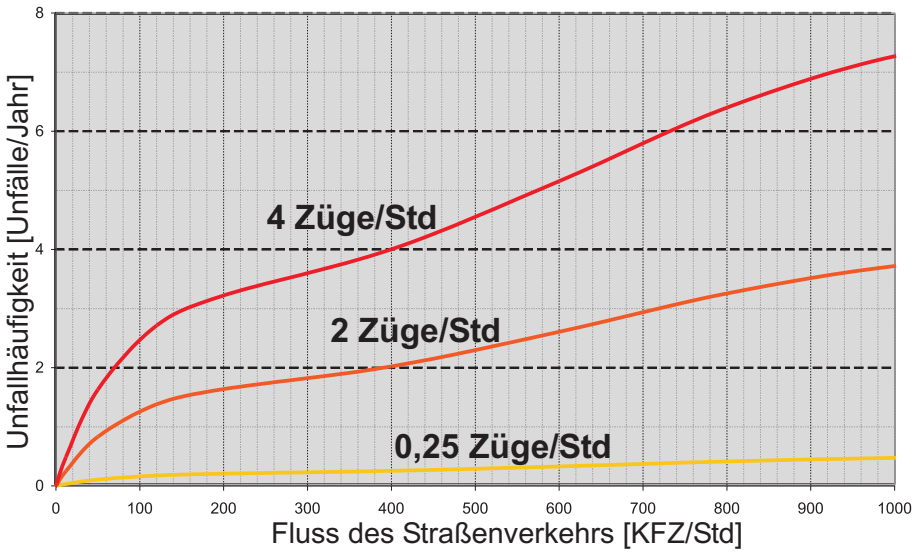

Abbildung 7.11: Kollektives Risiko als Unfallhäufigkeit in Abhängigkeit von den Verkehrsflüssen an einem ungesicherten Bahnübergang

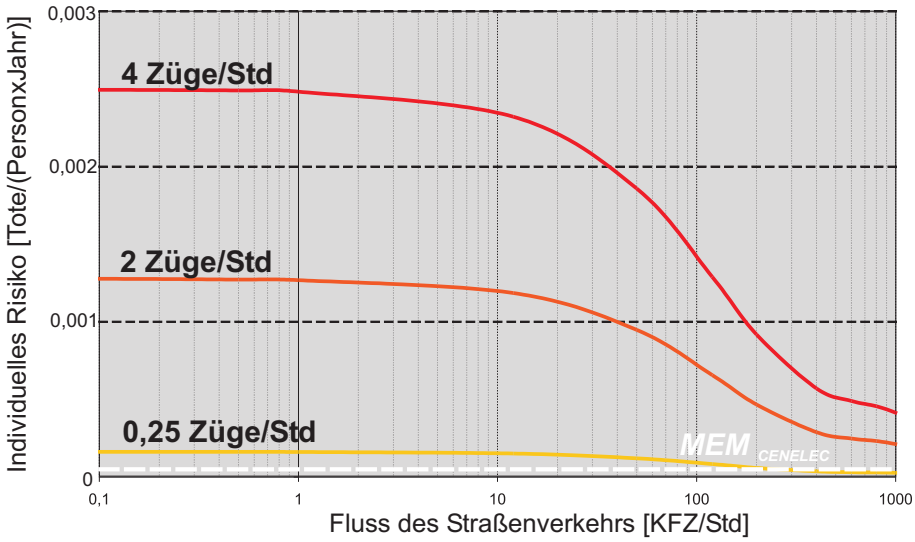

Abbildung 7.12: Individuelles Risiko in Abhängigkeit von den Verkehrsflüssen an einem ungesicherten Bahnübergang

schwach befahrenen Straßen (Feldwegen) ein unproportional hohes individuelles Risiko aufweisen.
Der Vergleich mit dem durch das Akzeptanzkriterium MEM zulässigen individuellen Risiko zeigt, dass eine Risikoreduktion durch ein technisches System (Bahnübergangsicherungsanlage) ab bestimmten Größen der Verkehrsvolumen unbedingt notwendig ist.

7.4 Bildung und Analyse des Modells der BÜ-Systemfunktionalität

7.4.1 Modellbildung

Die einzige betriebliche Funktion der Bahnübergangsicherungsanlage (BÜSA) ist, die Straßenverkehrsteilnehmer rechtzeitig vor dem Eintreffen eines Zuges zu warnen. Abbildung 7.13 zeigt die Anbindung der Systemfunktionalität in das Modell des Betriebsprozesses auf dem Bahnübergang (aus der Abb. 7.7). Der Platz *LC-protection-intact* stellt dabei die funktionale Ressource der gesamten BÜSA Funktionalität dar.

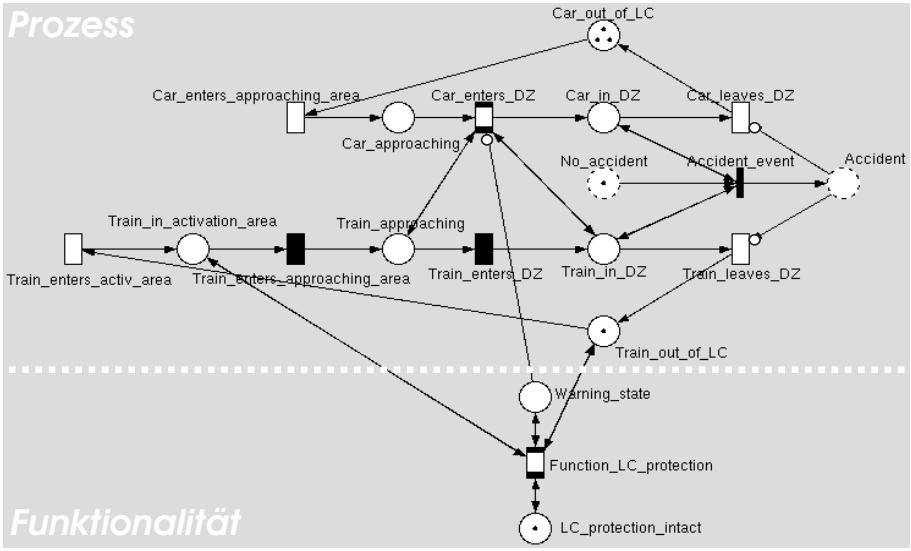

Abbildung 7.13: Prozessfunktionales Modell des gesicherten Bahnübergangs

Die Dauer der Einleitung des Sicherungsvorgangs, die von der technischen Ausstattung der BÜSA abhängt, fordert eine Erweiterung des Prozessmodells des Eisenbahnverkehrs um einen "Aktivierungsbereich", repräsentiert durch den Platz *Train-in-activation-area*. Der zeitliche Parameter der deterministischen Transition *Train-enters-approaching-area* T_{activ}, der die Aufenthaltsdauer in diesem Bereich vorgibt, ergibt sich aus

$$T_{active} = T_{tech} - T_{approach} \tag{7.1}$$

wobei T_{tech} der technischen Ankündigungszeit des modellierten Bahnübergangstypen entspricht und $T_{approach}$ der Zeitparameter der Transition *Train-enters-DZ* ist (stellt die Aufenthaltszeit des Zuges im Sichtbereich des KFZ-Fahrers dar).
Die eigentliche Warnung der BÜSA ist durch den Platz *Warning-state* modelliert, der Einfluss seiner Markierung auf das Verhalten der KFZ-Fahrer (beschrieben in der Instanz *Car-enter-DZ*) ist durch einen Inhibitor dargestellt.
Abbildung 7.14 zeigt die Verfeinerung der Instanz *Function-LC-protection*, die die grundsätzlich notwendige Funktionalität einer BÜSA vereinfacht beschreibt (s. Unterkapitel 7.1.1). Die Aktivierung der Warnung erfolgt durch die Markierung des Platzes *Train-in-activation-area* und wird durch die Markierung des Platzes *Train-out-of-LC* beendet.

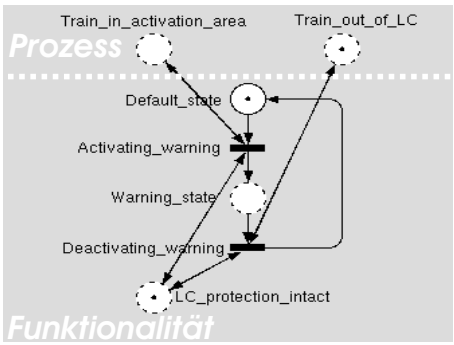

Abbildung 7.14: Grundsätzliche Funktionalität der Bahnübergangsicherungsanlage

Abbildung 7.15 zeigt detailliert den Einfluss der Warnung der BÜSA auf das Verhalten der KFZ-Fahrer. Wie ersichtlich ist, verhindert die Markierung des Platzes *Warning-state* die Einfahrt in den Gefahrenbereich aller bislang modellierten Gruppen der KFZ-Fahrer durch entsprechende Inhibitoren. Andererseits wird eine neue Fahrergruppe betrachtet (IV), die das Verhalten der KFZ-Fahrer modelliert, die zwar die Warnung der BÜSA wahrnehmen, sich jedoch nach einer bestimmten Wartezeit (ohne einen Zug im Sichtbereich) entscheiden, diese zu ignorieren und in den Gefahrenraum des BÜ einfahren (angenommen wird hierbei, dass es sich nicht um eine BÜ-Sicherung durch Vollschranke handelt).
Die Gruppe dieser Warnungen ignorierenden Fahrer (IV) existiert nur bei aktiver Warnung der BÜSA (modelliert durch die Testkante zwischen dem Platz *Warning-state* und der kausalen Transition *Car-enters-Warning-no-train*), dagegen werden in diesem Falle die Fahrergruppen II und III nicht betrachtet. Der prozentuale Anteil der Fahrergruppe IV gegenüber der Gruppe der korrekten Fahrer I, ist durch die Gewichtung

W4 gegeben. Sein Beispielwert *W4=0.3* stellt die Situation dar, in der das Verhältnis der KFZ-Fahrergruppe IV zu der Fahrergruppe I dem Wert 23% (erhalten durch 0,3/(1+0,3)) entspricht.

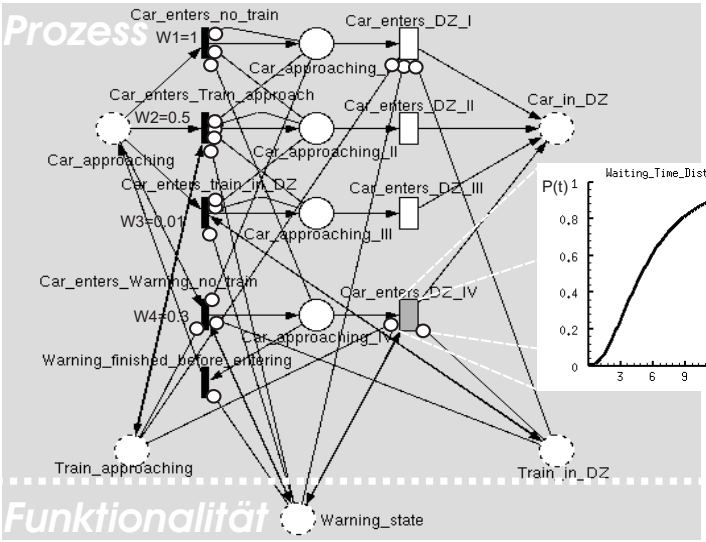

Abbildung 7.15: Modellierung des Verhaltens der KFZ-Fahrer am gesicherten Bahnübergang

Die eigentliche Wartezeit der KFZ-Fahrer der Gruppe IV ist durch die allgemeine stochastische Transition *Car-enters-DZ-IV* modelliert. Die hinterlegte stochastische Verteilung kann aus statistischen Daten und Verhaltenbeobachtungen [Vijendran et al. 2004] ermittelt werden. Das Verhalten der Autofahrer der Gruppe IV nach dem Erlöschen der Warnung ist durch die kausale Transition *Warning-finished-before-entering* gegeben.
Die Anwesenheit einer Bahnübergangsicherungsanlage selbst ändert das Verhalten der KFZ-Fahrer auch in dem Sinne, dass bei ihrem Grundzustand (Warnung ausgeschaltet) die Einfahrt der Straßenfahrzeuge in den Gefahrenraum wesentlich wahrscheinlicher ist als bei einem ungesicherten Bahnübergang. Deswegen wurden die Gewichtsfaktoren der Fahrergruppen II und III entsprechend erhöht (im Beispiel um eine Zehnerpotenz).

7.4.2 Analyse

Qualitative Analyse Abbildung 7.16 zeigt den Graphen von Mengen globaler sicherheitsrelevanter Zustände des um die Funktionalität der BÜSA erweiterten Prozessmodells. Die Definition der gefährlichen Situationen wurde um die Gefahr ergänzt, wenn sich vor dem BÜ-Gefahrenraum ein KFZ-Fahrer befindet, der die Missachtung

der Warnung beabsichtigt. Die ermittelten Zustandsübergänge konnten zur Modellverifikation und -validation verwendet werden.

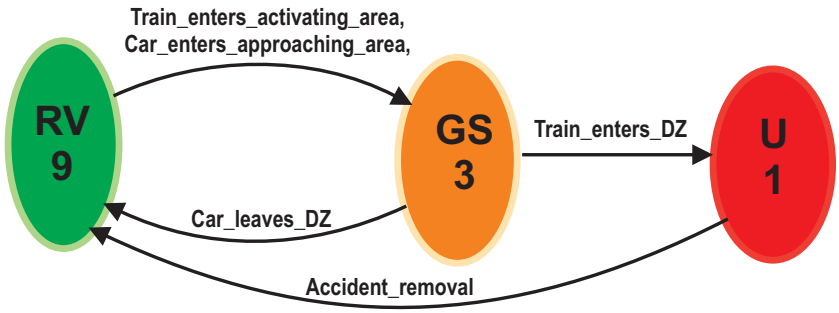

Abbildung 7.16: Graph von Mengen globaler sicherheitsrelevanter Zuständen des modellierten gesicherten Bahnübergangs

Weil das Modell eine Möglichkeit des zeitlich unbegrenzten Aufhaltens der Straßenfahrzeuge im Gefahrenraum, sowie die potentielle Missachtung der BÜSA-Warnung durch KFZ Fahrer betrachtet, konnte keine vollständige Eliminierung der gefährlichen Situationen und des Unfallzustandes erreicht werden. Dies wäre der Fall wenn die grundsätzliche Funktionalität der BÜSA um eine Funktion der Gefahrenraumfreimeldung und durch Ergänzung der Warnung durch eine vollständige Sperrung der Einfahrtmöglichkeit (z.B. durch eine Vollschranke) erweitert würde.
Den genaueren Einfluss der ergänzten Systemfunktionalität auf die Reduktion des betrieblichen Risikos zeigt die quantitative Modellanalyse.

Quantitative Analyse Abbildung 7.17 zeigt den Verlauf des betrieblichen Risikos an einem mit der Grundfunktionalität der BÜSA ausgestatteten Bahnübergang. Als Bezugsgröße wurde in diesem Fall die Länge der technischen Ankündigungszeit T_{tech} genommen, während der die KFZ-Fahrer schon vor der Ankunft des Zuges gewarnt werden. Als Beispiel sind hier die Verkehrsflüsse von 120 KFZ/Std und 2 Züge/Std. angenommen worden.
Dargestellt ist die deutliche Senkung des betrieblichen Risikos im Falle der Verlängerung der technischen Ankündigungszeit solange keine Missachtung der BÜ-Warnung betrachtet wurde (grüne Linie). Für die angenommenen betrieblichen und geographischen Verhältnisse des BÜ erreicht das individuelle Risiko der Straßenverkehrsteilnehmer den akzeptierbaren Wert (im Sinne des MEM Kriteriums) bei einer Ankündigungszeit von ca. 42 s. Die modellierte funktionale Spezifikation der BÜSA ist daher ausreichend, um die notwendige Reduktion des betrieblichen Risikos zu erreichen, und kann zur weiteren Analysen der funktionalen Verlässlichkeit verwendet werden.

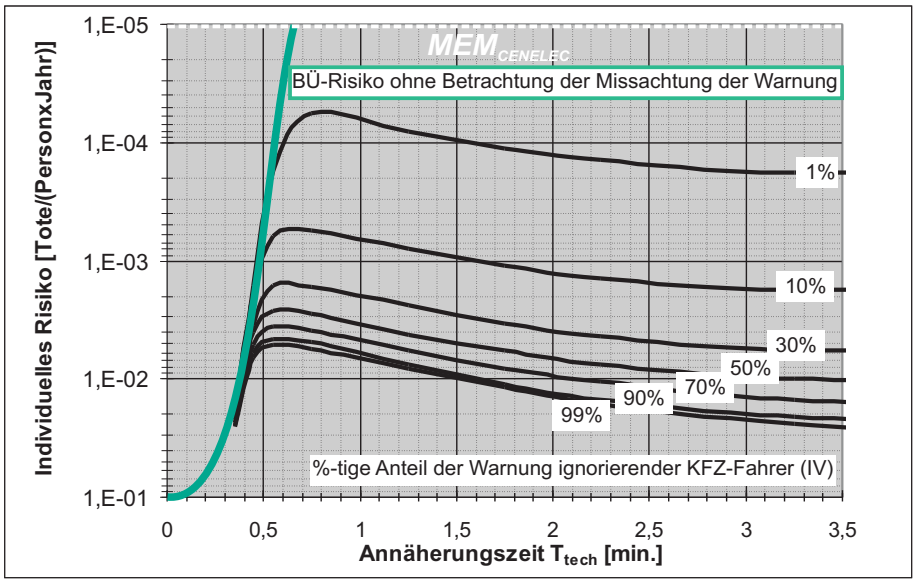

Abbildung 7.17: Abhängigkeit des betrieblichen Risikos von der Länge der Ankündigungszeit für die BÜ-Warnung

Im Weiteren zeigt der Graph aber auch deutlich, wie das betriebliche Risiko bei Verlängerung der Ankündigungszeit über 50 s im Falle der betrachteten Missachtung der Warnung durch die KFZ-Fahrer steigt. Der Anstieg ist desto stärker je höher der Anteil der Warnung missachtender KFZ-Fahrer angenommen wird (die prozentuelle Proportion entspricht dem Gewichtsfaktor der Fahrergruppe IV). Dieser Verlauf bestätigt auch die sinnvolle Praxis einiger europäischer Bahnen, einen Bahnübergang, der länger als 3 Minuten verschlossen ist, als ungesichert zu betrachten.

Die Ergebnisse zeigen, dass eine Integration der Missachtung der Verkehrsregel durch die KFZ-Fahrer es nicht ermöglicht, durch die gegebene Funktionalität der BÜSA die gewünschte Risikoreduktion zu erreichen. Aus diesem Grund wird diese Art des potentiellen menschlichen Verhaltens aus der Sicherheitsanalyse herausgenommen und es werden nur die durch den Systemausfall verursachten Gefahren betrachtet. Diese Art der Ergebnisse kann zur Beurteilung der Risikoreduktion verschiedener technischer und legislativer Maßnahmen angewendet werden.

7.5 Bildung und Analyse des Modells der BÜ-Systemfunktionsverlässlichkeit

Die bisher vorgestellte Modellierung basierte auf der Annahme der fehlerfreien Funktionalität aller modellierten Systemfunktionen der BÜSA. Der nächste Schritt der Sicherheitsanalyse im Sinne der behandelten *PROFUND*-Methode ist die Betrachtung des potentiellen Verlässlichkeitsverhaltens der beteiligten funktionalen Ressourcen mit dem Ziel, anhand der Evaluation des resultierenden betrieblichen Risikos die funktionalen Sicherheitsziele der BÜSA zu ermitteln.

7.5.1 Modellbildung

Abbildung 7.18 links zeigt die Erweiterung der Modellierung der Systemfunktionalität (aus Abb. 7.14) um die Funktionsverlässlichkeit in Form einer Instanz *LC-protection-dependability*. Eine Verfeinerung dieser Instanz zeigt Abbildung 7.18 rechts.

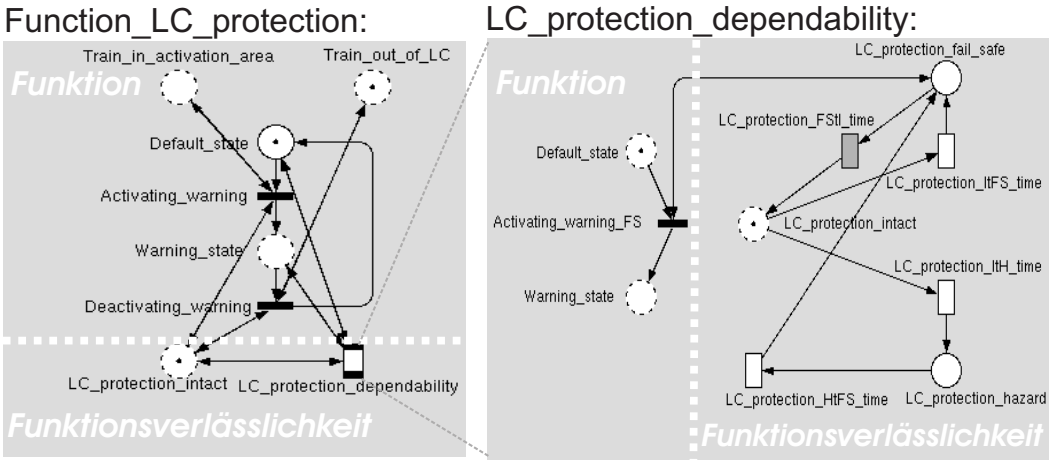

Abbildung 7.18: Ergänzung der BÜSA-Funktionalität durch ihre Verlässlichkeitsmodellierung

Da das Ausbleiben der Funktion der BÜSA für den Betrieb eine Gefahr darstellt, wurde die Modellierung ihres Verlässlichkeitsverhalten im Sinne der allgemeinen Beschreibung der Verlässlichkeit einer hazard-passiven Funktion durchgeführt (Abb. 5.21). Dabei wurde lediglich die Möglichkeit eines zeitbedingten gefährlichen und eines sicheren Ausfalles der BÜSA betrachtet (modelliert durch die Transitionen *LC-protection-ItH-time* und *LC-protection-ItFS-time*).
Die Möglichkeit der Erkennung des gefährlichen Zustandes der BÜSA (Hazards) bildet die Transition *LC-protection-HtFS-time*. Der Zeitparameter dieser Transition ergibt

sich aus den Charakteristiken des Eisenbahnverkehrs, wo die Hazarderkennung z.B. durch einen Lokführer in Frage kommt. Unter Betrachtung des längsten Abstandes zwischen zwei hintereinander folgenden Zügen wurde die Hazarderkennungszeit von 8 Std angenommen.
Die Erkennung des Hazardzustandes führt zu einem sicheren Fehlerzustand (Fail-safe Zustand) der BÜSA, in dem, als eine von mehreren in der Praxis genutzten Möglichkeiten, die Warnung für den Straßenverkehr eingeleitet wird (modelliert durch die kausale Transition *Activating-warning-FS*). Die Beseitigung des fail-safe Zustandes der BÜSA erfolgt nach der Reparaturzeit (beim betrachteten Mittelwert von 2 Std), die durch eine allgemeine stochastische Verteilung der Transition *LC-protection-FStI-time* modelliert wurde.

7.5.2 Analyse

Qualitative Analyse Abbildung 7.19 zeigt den Graphen der Mengen globaler sicherheitsrelevanter Zustände des um die Systemverlässlichkeit erweiterten prozessfunktionalen Modells. Bedingt durch die Erweiterung, sind in den Graphen die Menge des globalen Hazard- und Fail-Safe-Zustandes der BÜSA integriert worden.
Aus der Abbildung ist ersichtlich, dass durch die Modellerweiterung auch die Komplexität des zugehörigen Erreichbarkeitsgraphen gestiegen ist (insgesamt 73 Zustände). Die ermittelten Übergänge zwischen dem Regelverhalten und den Systemverlässlichkeitszuständen (H und FS) bestätigen die Korrektheit der Modellierung. Der Vergleich der ermittelten Übergangstransitionen zu Mengen gefährlicher Situationen und zu Unfallzuständen mit dem entsprechenden Graphen des prozessfunktionalen Modells (Abb. 7.16) und des Ereignisbaums (Abb. 7.3) kann zu weiterer Verifikation und Validation verwendet werden.

Quantitative Analyse Die Aufgabe der quantitativen Analyse ist es, den Einfluss des Verlässlichkeitsverhaltens der BÜSA auf das resultierende betriebliche Risiko sowie auch auf die betriebliche Systemverfügbarkeit zu untersuchen.
Abbildung 7.20 zeigt den Verlauf des betrieblichen Risikos in Abhängigkeit von der Rate des gefährlichen Ausfalles der BÜSA. Die Auswertung wurde für zwei mögliche Werte der technischen Ankündigungszeit durchgeführt (42 s und 54 s).
Die dargestellten Analyseergebnisse bestätigen, dass die maximal mögliche Reduktion des betrieblichen Risikos stark von der Länge der technischen Ankündigungszeit abhängig ist (s. auch Abb. 7.17, ohne Betrachtung der Möglichkeit der Warnungsmissachtung durch die KFZ-Fahrer). Beim Vergleich mit dem durch das Kriterium MEM akzeptierbaren individuellen Risiko zeigt sich auch der Bezug der technischen Ankündigungszeit mit dem notwendigen Sicherheitslevel (SIL) der einzusetzenden BÜSA. In

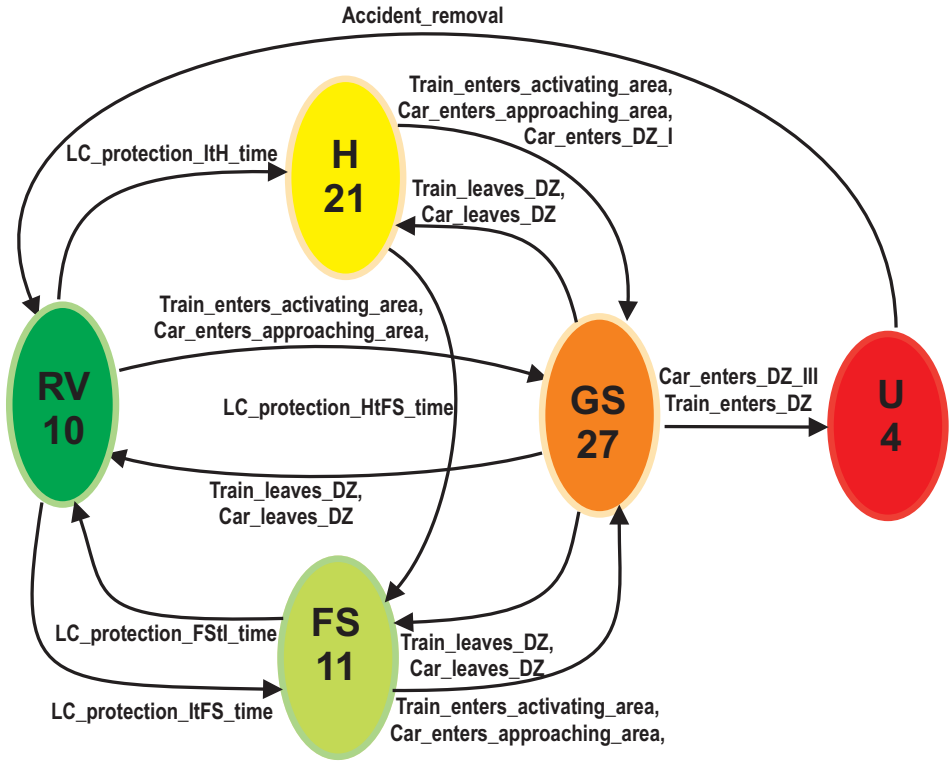

Abbildung 7.19: Graph der Mengen globaler sicherheitsrelevanter Zustände des Prozess-Funktions-Verlässlichkeitsmodells des gesicherten BÜ

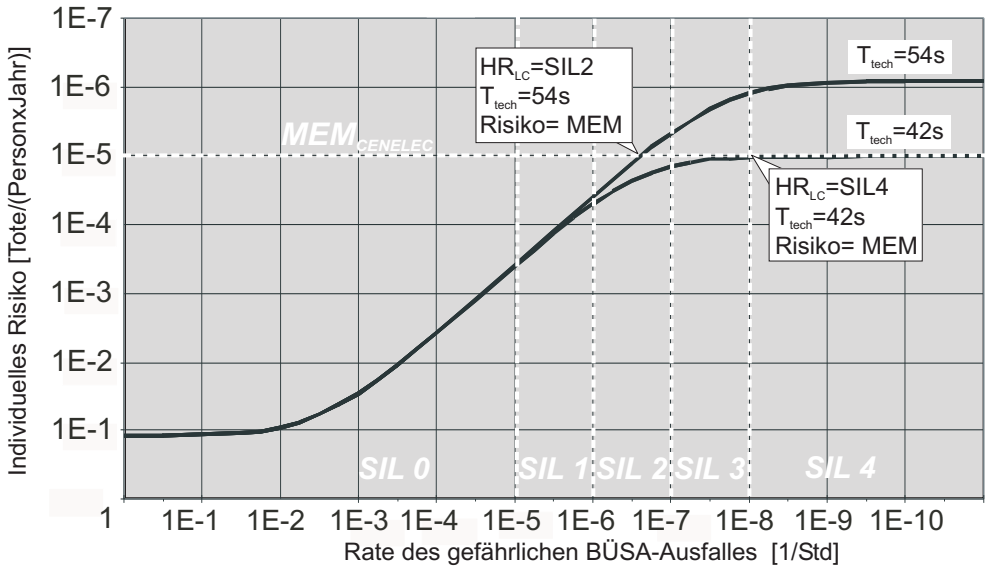

Abbildung 7.20: Modellierung des Verhaltens der KFZ-Fahrer am gesicherten Bahnübergang

diesem Beispiel ermöglicht die Verlängerung der Ankündigungszeit von den minimalen 42 s auf 54 s die BÜSA anstatt mit SIL 4 mit einem System von SIL 2 auszurüsten.

Abbildung 7.21 zeigt den möglichen Einfluss der Rate des sicheren Ausfalles der BÜSA. Da der sichere Ausfall eine dauerhafte Warnung für den Straßenverkehr bedeutet, ist es sehr wahrscheinlich, dass es zu seiner wiederholten Missachtung durch die KFZ-Fahrer kommen wird. Die Analyse des integrierten Modells des menschlichen Verhaltens am Bahnübergang zeigt, dass ein öfter vorkommender Fail-Safe-Ausfall (z.B. $1,3 \times 10^{-3}$ pro Std) ein höheres Sicherheitsniveau der BÜSA verlangt (SIL 3 anstatt SIL 2).

Ein ganzheitlicher Überblick über den Einfluss der Systemverlässlichkeit inklusive seiner funktionalen Parameter (hier die technische Ankündigungszeit) auf die betriebliche Sicherheit sowie auch auf die betriebliche Verfügbarkeit kann durch die Darstellung in Form des Verfügbarkeit/Sicherheit (V/S) Diagramms gewonnen werden [Schnieder 2003]. Abbildung 7.22 zeigt ein solches Diagramm für das betrachtete Beispiel des gesicherten Bahnübergangs, ohne Betrachtung des unkorrekten menschlichen Verhaltens.

Das ermittelte V/S Diagramm bestätigt die Tatsache, dass die Erhöhung der Sicherheit oft auf Kosten der Verfügbarkeit realisiert wird. Eine BÜSA ist ein typisches Beispiel solcher Sicherungssysteme, dessen Warnzustand bzw. Fail-Safe-Zustand für den Straßenverkehr eine Unverfügbarkeit des Verkehrsweges darstellt. Dagegen ist die Unverfügbarkeit eines ungesicherten Bahnübergangs nur durch die tatsächliche Anwesenheit des Zuges im Gefahrenraum bzw. Annäherungsbereich gegeben.

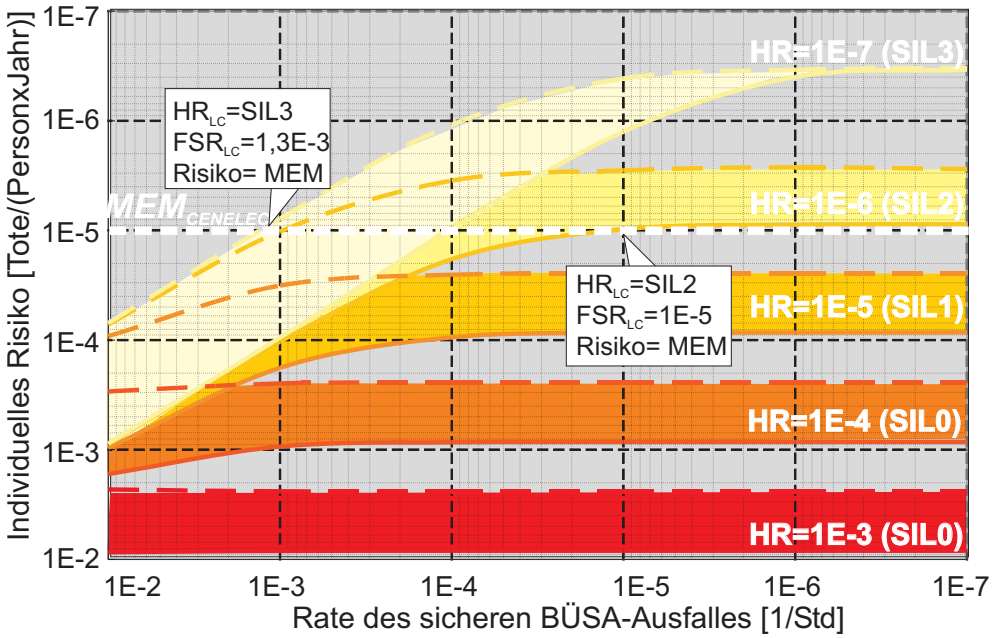

Abbildung 7.21: Individuelles Risiko der KFZ-Fahrer in Abhängigkeit von den Raten der sicheren und der gefährlichen Ausfälle der BÜSA

Die Darstellung durch das V/S Diagramm kann auch innerhalb weiterer Analysen sinnvolle Verwendung finden, so z.B. in der Phase der Suche nach einer geeigneten Implementierung der geforderten Systemfunktionalität durch unterschiedliche bahnübergangstypische Sicherungsarten.

Funktionale Sicherheitsanforderungen Das Ergebnis der qualitativen und quantitativen Analyse bildet die Definition der funktionalen Sicherheitsanforderungen für die BÜSA, die in diesem Beispiel als globale Ressource aller genannten Funktionen betrachtet wurde.

Unter Berücksichtigung der vorgestellten quantitativen Auswertungen in Abbildungen 7.20, 7.21 und 7.22 scheint die optimale tolerierbare Rate des gefährlichen Ausfalls der BÜSA der Wert $THR_{BUSA} = 4 \times 10^{-7}$ Ausfälle pro Std (SIL 2) zu sein. Eine Voraussetzung dieses Wertes ist im betrachteten Beispiel die minimale Länge der technischen Ankündigungszeit von 54 s und eine maximale Rate der sicheren Ausfälle von $TFSR_{BUSA} = 1 \times 10^{-5}$ Ausfällen pro Std.

Der ermittelte Wert der tolerierbaren gefährlichen Ausfallrate von SIL 2 entspricht den praktizierten Sicherheitsanforderungen an ein Bahnübergangsicherungssystem ähnlicher Art in einigen Länder Europas wie z.B. Schweden, Tschechien oder Slowakei.

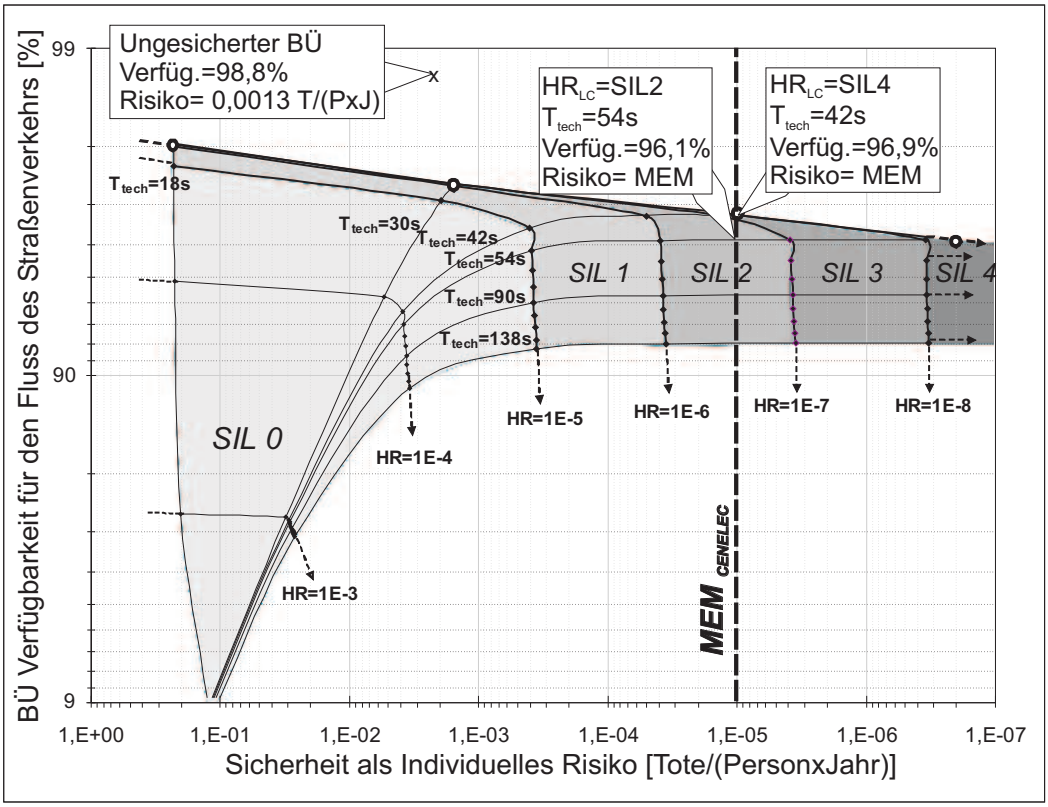

Abbildung 7.22: V/S Diagramm des modellierten gesicherten Bahnübergangs

7.6 Bildung und Analyse des Modells der BÜ-Systemimplementierung

Im Gegensatz zu der allgemeinen Betrachtung der Funktionsmodellierung zielt die Modellbildung der Systemimplementierung darauf, die konkrete technische Systemumsetzung zu beschreiben und ihren Einfluss auf die gesetzten funktionalen Sicherheitsziele zu untersuchen. Dank der überschaubaren Komplexität des Beispiels Bahnübergang kann in diesem Fall die Modellierung der Systemimplementierung als Verfeinerung der bereits beschriebenen Funktionalität vorgenommen werden. Auf diese Weise kann neben der Erfüllung der funktionalen Sicherheitsziele auch die erreichte Reduktion des Risikos im Eisenbahnbetrieb überprüft werden.

7.6.1 Modellbildung

Im Sinne der Systemdefinition (Unterkapitel 7.1.1) wurden zur Implementierung der fünf grundsätzlichen Funktionen einer BÜSA die folgenden vier technischen Komponenten vorgesehen:

- Ein Achszähler zur Realisierung der Funktion Zugdetektion (*Train-detection*)
- Eine elektronische Steuerungseinheit zur Realisierung der Funktion Aktivierung und Deaktivierung der BÜSA (*LC-control*)
- Ein Lichtzeichen zur Realisierung der Funktion Warnung des Straßenverkehrs (*Warning*)
- Ein Fahrzeugsensor zur Realisierung der Funktion Erkennung der Räumung des BÜ-Gefahrenbereichs (*Train-leaving-detection*)

Abbildung 7.23 zeigt die Zuordnungsrelation der funktionalen Ressource der BÜSA, repräsentiert durch den Platz *Function-LC-protection*. Die vier darauf liegenden Marken bilden die Anwesenheit der vier genannten technischen Komponenten ab, die die Funktionalität der BÜSA implementieren.
Abbildung 7.24 oben zeigt die Modellierung der Funktionsimplementierung als Verfeinerung der Instanz *Function-LC-protection* aus Abbildung 7.13. Die Ankopplung des Implementierungsmodells an das Modell des BÜ-Betriebsprozesses erfolgt durch die Portplätze *Train-in-activation-area*, *Train-out-of-LC* und *Warning* (entsprechend der Modellierung der Systemfunktionalität in Abb. 7.14).
Ähnlich wie bei der Modellierung der Systemfunktionalität kann auch die Funktionsimplementierung um die Verlässlichkeit ihrer Ressourcen erweitert werden. Zur Beschrei-

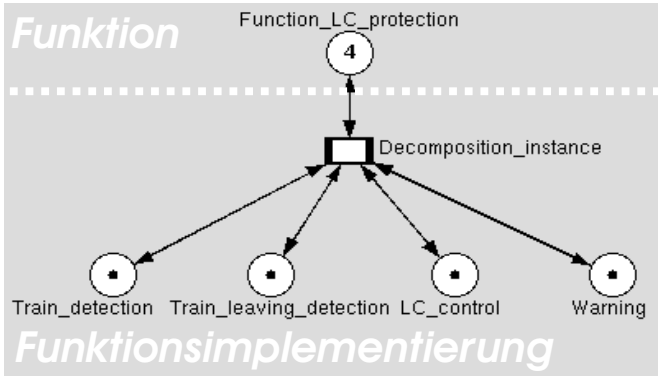

Abbildung 7.23: Zuordnungsrelation der funktionalen Ressource BÜSA

bung des Verlässlichkeitsverhaltens dieser Implementierungsressourcen können ebenfalls die allgemeinen Verlässlichkeitsmodelle der hazard-aktiven und hazard-passiven Implementierungsfunktionen angewendet werden (s. Abbildungen 5.20 und 5.21).
Der obere Teil der Abbildung 7.24 beinhaltet bereits die Ankopplung der Funktionsimplementierung an die Modelle der Implementierungsverlässlichkeit, die durch die entsprechenden Instanzen repräsentiert sind. Ihre Verfeinerung befindet sich im unteren Teil der Abbildung.
In die Betrachtung des Verlässlichkeitsverhaltens des Achszählers (*Train-detection-dependability*) wurde lediglich der gefährliche Ausfall gezogen (modelliert durch Transition *Train-det-ItH-time*). Die Erkennung dieses Ausfalles nach der durch die Transition *Train-det-HtI-time* repräsentierten stochastisch verteilten Zeit führt direkt zum Betriebszustand dieser Komponente.
Ähnlich vereinfacht wurde die Modellierung des Fahrzeugsensors (*Train-leaving-detection-dependability*), wobei hier nur sein sicherer Ausfall betrachtet wurde (modelliert durch Transition *Train-leaving-det-ItFS-time*).
Komplexer ist die Modellierung des Verlässlichkeitsverhaltens der elektronischen Steuerungseinheit (*LC-control-dependability*), die sowohl einen sicheren als auch einen gefährlichen Ausfall betrachtet (modelliert durch Transition *LC-control-ItH-time* und *LC-control-ItFS-time*). Die Erkennung des gefährlichen Ausfalls führt zum sicheren Zustand der Steuerung, der sich als eine Aktivierung in der Funktionsimplementierung äußert (modelliert durch die kausale Transition *LC-control-activation-FS*).
Die Verlässlichkeitsmodellierung der Warnung (*Warning-dependability*) geht davon aus, dass jede Fahrtrichtung des Straßenverkehrs mit zwei Lichtzeichen ausgestattet ist. Diese Anordnung bildet eine Art Redundanz, wobei es sich aus Sicht der Verlässlichkeitsbetrachtung um einen gefährlichen Warnungsausfall erst bei einem gleichzeitigen Ausfall beider Lichtzeichen handelt. Diese nur potenziell gefährliche Ausfallfolge wurde durch

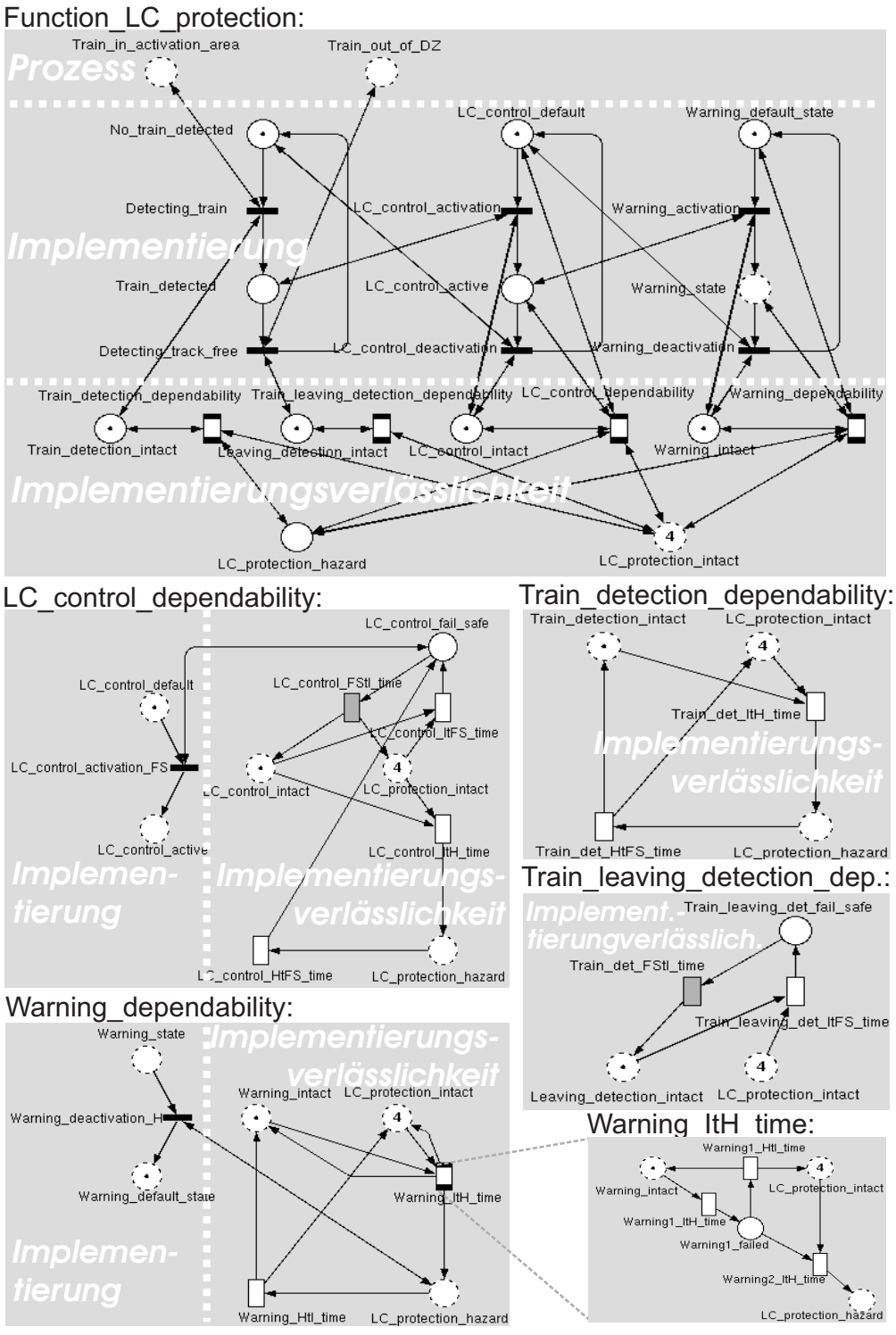

Abbildung 7.24: Modellierung der Funktionsimplementierung und Implementierungsverlässlichkeit der mit einem Lichtzeichen ausgerüsteten BÜSA

ein separates Unternetz modelliert (*Warning-ItH-time*), in dem der Ausfall des ersten Lichtzeichens (Transition *Warning1-ItH-time*) vor einem zweitem Lichtzeichenausfall (Transition *Warning2-ItH-time*) erkannt werden kann (Transition *Warning-HtI-time*). Im anderen Fall wird der Hazardzustand erreicht, der auf der Funktionsimplementierungsebene die Ausschaltung der Warnung erzwingt (durch die kausale Transition *Warning-deactivation-H*).
In der vorgestellten Modellierung der Implementierungsverlässlichkeit wurden der globale Betriebs- und der globale Hazardzustand der BÜSA (*LC-protection-intact* bzw. *LC-protection-hazard*) aus dem Modell der Systemfunktionalität beibehalten, wobei die einzelnen Ausfälle der Komponenten durch unterschiedliche farbige Marken repräsentiert sind. Diese Art der Modellierung vereinfacht die nachfolgende Verifikation und Validation des erstellten Modells.

7.6.2 Analyse

Qualitative Analyse Ziel der qualitativen Analyse ist nach wie vor eine Überprüfung der Korrektheit der Modellbildung. Es können hier alle beschriebenen Methoden wie interaktive Simulation, Bildung des Graphen der Mengen globaler Zustände, Invariantenanalyse oder die Bildung des Unfallbaumes erfolgreich eingesetzt werden.
Ein wichtiges Ergebnis aus der Bildung des Unfallbaumes ist die Identifikation der unabhängigen risikobeitragenden Ressourcen der BÜSA. Durch Anwendung des in den Unterkapiteln 6.2.1 und 6.2.3 vorgestellten Verfahrens kann gezeigt werden, dass von den zur Implementierung vorgesehenen Komponenten der Achszähler, die Steuerungseinheit und die Lichtzeichen das betriebliche Risiko unabhängig beeinflussen können. Der Ausfall des Fahrzeugsensors (zur Erkennung der Räumung des Gefahrenraums durch den Zug) fällt in diese Gruppe nur im Falle der Betrachtung einer möglichen Missachtung der Warnung durch die KFZ-Fahrer. In dem anderen Fall kann diese Komponente als nicht sicherheitsrelevant angesehen werden.
Durch die in diesem Beispiel beibehaltene Verbindung zum Modell des Betriebsprozesses kann der Einfluss des Verlässlichkeitsverhaltens einzelner Implementierungskomponenten auf das betriebliche Risiko auch durch die quantitative Analyse bestätigt werden.

Quantitative Analyse Durch die Verbindung des beschriebenen Modells des Betriebes, der Implementierungsfunktionalität und der Implementierungsverlässlichkeit mit dem Modell der Unfallfolgen (Abb. 7.5) kann unter Anwendung des Vorgehens aus Unterkapitel 6.2.3 die quantitative Analyse des betrieblichen Risikos als Sensitivitätsanalyse durchgeführt werden.

Abbildung 7.25 zeigt die Näherungsverläufe der Beiträge der einzelnen Implementierungskomponenten zum individuellen Risiko der Teilnehmer des Straßenverkehrs entsprechend ihren Hazardraten, wobei keine Missachtung der Warnung betrachtet wurde.

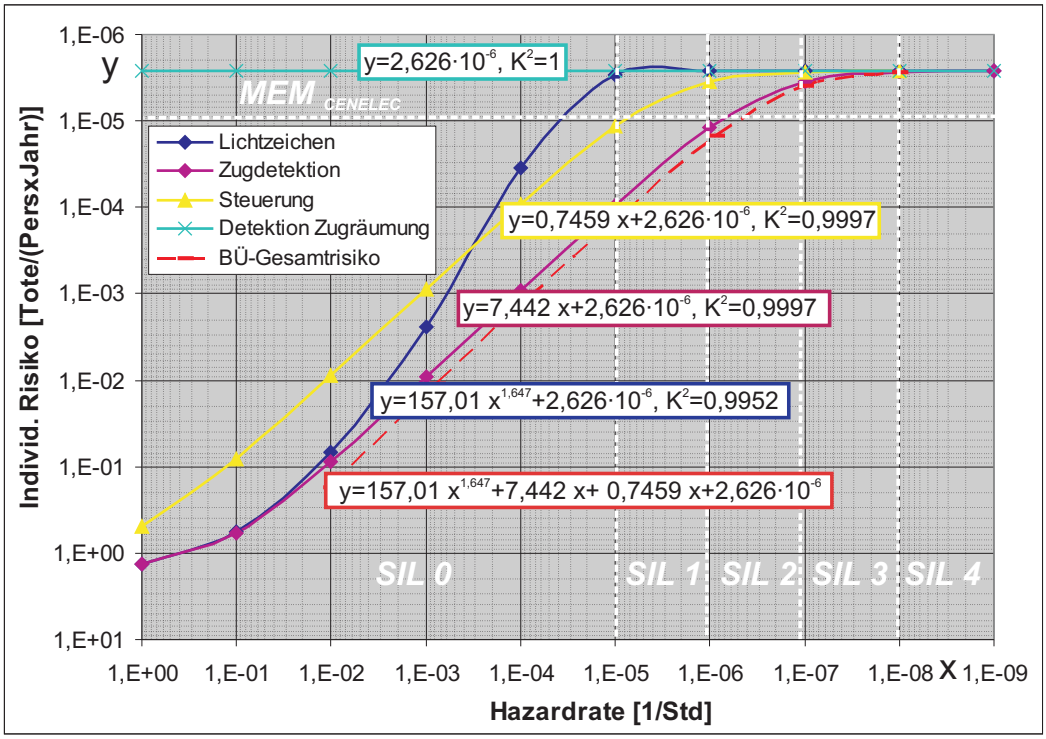

Abbildung 7.25: Das individuelle Risiko der Teilnehmer des Straßenverkehrs an einem BÜ in Abhängigkeit von der Rate gefährlicher Ausfälle der Implementierungskomponenten der BÜSA mit Näherungsgleichungen und Korrelationsfaktoren einzelner Verläufe

Wie ersichtlich ist, nähern sich alle dargestellten Risikocharakteristiken dem Wert von $2,626 \cdot 10^{-6}$ Tote/(Person x Jahr), was dem durch die Systemfunktionalität gegebenen Restrisiko entspricht (durch die verwendete technische Ankündigungszeit).
Die Analyse bestätigte, dass die Erkennung der Zugräumung in diesem Fall nicht als sicherheitsrelevant anzusehen ist. Als größ zeigt sich dabei der Risikobeitrag der Implementierungskomponente der Zugerkennung (aufgrund der strengen Annahme keiner sicheren Ausfälle), den niedrigsten weist die Warnung auf (aufgrund der Betrachtung seiner redundanten Ausführung).
Dank der Unabhängigkeit einzelner betrachteter Komponenten kann die resultierende Abhängigkeit des betrieblichen Risikos durch die Summe der einzelnen Risikobeiträge ausgewertet werden (s. Gleichung 6.9):

$$R_{BU} = R_{Lz} + R_{Ze} + R_{Stg} + R_F \tag{7.2}$$

Anhand der durchgeführten Näherung einzelner Risikoverläufe (s. Abb 7.25) konnte die folgende mathematische Abhängigkeit abgeleitet werden:

$$R_{BU} = 157,01 \cdot Hr_{Lz}^{1,647} + 7,442 \cdot Hr_{Ze} + 0,7459 \cdot Hr_{Stg} + 2,626 \cdot 10^{-6} \tag{7.3}$$

Die ermittelte Gleichung kann direkt zu der Optimierung und anschließenden Festlegung der Sicherheitsziele einzelner Implementierungskomponenten verwendet werden.

Sicherheitsanforderungen der Systemimplementierung Die Hazardraten der einzelnen Implementierungskomponenten Hr_{Lz}, Hr_{Ze} und Hr_{Stg} bilden den Vektor der Verlässlichkeitsparameter $\overrightarrow{p}$ des *PROFUND*-Modells des behandelten gesicherten Bahnübergangs. Eine risikoakzeptierbare Belegung dieses Vektors $\overrightarrow{p_{acceptable}}$ mit den zugehörigen Sicherheitsanforderungstufen (SIL) und den Werten des entsprechenden individuellen Risikos der Teilnehmer des Straßenverkehrs stellt die Tabelle 7.2 vor.

	THr [1/Std]	SIL	Ind. Risiko[T/(PxJ)]
Lichtzeichen	1,48E-05	0	4,37E-06
Achszähler	3,00E-07	2	6,03E-06
BÜ-Steuerung	2,00E-06	1	4,87E-06
Restrisiko			2,63E-06
Gesamtrisiko			**1,00E-05**

Tabelle 7.2: Sicherheitsanforderungen an die Komponenten der BÜSA Implementierung

Als Kriterium für die Suche der Parameter wurde in diesem Falle die Realisierung durch Komponenten der niedrigst möglichen Sicherheitsanforderungsstufe angewendet. Unter Kenntnis der entsprechenden Kostenfunktionen für die Herstellung und den Betrieb dieser Implementierungskomponenten könnte anhand der Gleichung 7.3 auch die kostenoptimale Belegung des Vektors $\overrightarrow{p_{costoptimal}}$ gefunden werden.
Die bekannten Sicherheitsanforderungen einzelner Implementierungskomponenten der BÜSA sind im weiteren auf die Subkomponenten zu verteilen. Als Beispiel kann hier die Architektur der BÜ-Steuerung genannt werden. Bei unausreichenden Sicherheitseigenschaften der Subsystemkomponenten sind geeignete strukturelle Maßnahmen wie Redundanz oder Überwachung zu entwerfen. Zu diesem Zweck können die typischen Modelle aus Unterkapitel 5.5.2 angewendet und im Sinne des Vorgehens aus den Unterkapiteln 6.3.2 und 6.3.1 analysiert werden.

Kapitel 8

Zusammenfassung und Ausblick

8.1 Zusammenfassung

Derzeit werden in den europäischen Ländern noch unterschiedliche organisatorische Strukturen, Strategien und betriebliche Regeln genutzt, um einen sicheren Eisenbahnverkehr zu gewährleisten. Der gemeinsame europäische Markt und die Anforderung an die Interoperabilität führen zum Bestreben nach Harmonisierung. Aus diesem Grund wurden von der CENELEC die ersten europäischen Normen erarbeitet, die die Verlässlichkeit im Sinne eines Oberbegriffes für Sicherheit, Zuverlässigkeit, Verfügbarkeit und Instandhaltbarkeit (RAMS) der Eisenbahnleit- und -sicherungssysteme betreffen. Im Gegensatz zum früher eher absoluten Verständnis der Sicherheit, basiert die neue Definition der Normen auf der Akzeptanz eines zulässigen Risikos des Eisenbahnbetriebes. Es ist die Aufgabe der Sicherheitsanalyse, das betriebliche Risiko zu ermitteln und auf seiner Basis die Anforderungen und Sicherheitsziele an die, den Betrieb steuernden und sichernden technischen Systeme zu definieren.

Die geltenden Normen sind allgemein gefasst und schreiben nicht konkret ein methodisches Vorgehen oder Regeln zur Ableitung von Sicherheitsanforderungen für Systemkomponenten aus dem zulässigen betrieblichen Risiko vor. Für diese Herleitung wird nur eine Reihe von mehr oder weniger formalen Techniken empfohlen und mit unterschiedlichem Erfolg eingesetzt. In den einzelnen Entwicklungsschritten werden meist verschiedene Systemmodelle und Beschreibungsmittel verwendet. Diese sind oft nicht systematisch ineinander überführbar, was das Risiko von Entwicklungsfehlern deutlich erhöht und die Nachvollziehbarkeit und die Transparenz des Entwurfs verringert.

Um eine ausreichende Genauigkeit der Risikobewertung zu erreichen, ist ein holistischer Ansatz der Beschreibung aller beitragenden Risikofaktoren notwendig. Das grundlegende Konzept der in dieser Arbeit angewendeten *PROFUND*-Methode zur Sicherheitsanalyse von Eisenbahnsystemen sieht vor, für alle Einflussfaktoren des Risikos im

Eisenbahnbetrieb ein einziges formales Beschreibungsmittel zu verwenden. Dieses betrifft einerseits den gesteuerten Verkehrsprozess (Process), in welchem das Potential für den Auftritt von unerwünschten Ereignissen besteht, anderseits die Funktionalität (Functionality) und Verlässlichkeit (Dependability) des untersuchten Eisenbahnleit- und -sicherungssystems.
Ziel dieser Arbeit war es zu zeigen, wie die Nutzung eines formalen Beschreibungsmittels die risikobasierte Sicherheitsanalyse methodisch unterstützen kann. Als geeignete formale Notation wurden Petrinetze gewählt. Diese Wahl wurde einerseits durch einen ausgereiften mathematischen Hintergrund und breite Analysemöglichkeiten begründet, die bereits zu vielen praktischen Anwendungen geführt haben, andererseits durch deren Universalität. Das wichtigste Ziel der Arbeit war es, die methodische Anwendung des Beschreibungsmittels dem Leser so nahe wie möglich zu bringen. Neben der Darstellung des Nutzungspotentials der formalen Herangehensweise, wurde darauf geachtet, den Bezug zum traditionellen Vorgehen beizubehalten und den formalen Ansatz als seine mögliche Erweiterung mit erkennbarem Mehrwert zu sehen.
Die Arbeit zeigt im Detail, wie Petrinetze einerseits zur Beschreibung der Unfallschwere und andererseits der Unfallursachen aus dem Eisenbahnbetrieb, der Systemverlässlichkeit oder der Systemimplementierung eingesetzt werden können. Die parallele Anwendung der einzelnen Schritte des vorgestellten methodischen Vorgehens an Beispielen aus dem Eisenbahnbereich unterstützt die allgemeingültigen Ausführungen mit praxisnahen Erklärungen.

8.2 Ausblick

Die weiterführenden Arbeiten sind insbesondere im Bereich der Entwicklung einer geeigneten Werkzeugunterstützung, einer domänenspezifischen Verfeinerung der Methode und weiterer Validationen der vorgestellten Methode durch praktische Anwendung vorgesehen.
Den wichtigsten Forschungs- und Entwicklungsbedarf stellt die Implementierung einer maßgeschneiderten Toolunterstützung dar. Die Hauptanforderung ist es dabei, dem Anwender zu ermöglichen, alle Schritte des vorgeschlagenen methodischen Vorgehens in einer Softwareumgebung durchführen zu können.
Eine bessere Akzeptanz des vorgestellten methodischen Vorgehens kann durch eine weitere Spezialisierung im Anwendungsbereich erreicht werden. Ein Beitrag dazu könnte die Modellierung von allen typischen bahnspezifischen Verkehrsabläufen, Systemfunktionalitäten und Funktionsimplementierungen leisten, die bei der Sicherheitsanalyse als Vorlage zur Parametrierung im Sinne des jeweiligen Anwendungsfalls genutzt werden könnte. Ein ideales Entwicklungsniveau wäre erreicht, wenn die eigentlichen Petrinetz-

module bestimmte Aufbaublöcke bilden würden, die der Anwender ohne Kenntnis der formalen Sprache parametrieren und zur gewünschten fallspezifischen Zusammensetzung anordnen könnte.
Ein weiterer algorithmischer Bedarf liegt in der Weiterentwicklung der vorgestellten Transformationsalgorithmen zu den traditionellen Beschreibungsmitteln der Sicherheitsanalyse. Hierzu gehört insbesondere die quantitative Parametrierung der generierten Graphen der Mengen globaler Zustände und Unfallbäume, die durch Verbindung mit der Modellanalyse realisiert werden könnte.
Eine Herausforderung stellt auch die Kopplung der quantitativen Modellanalyse mit Optimierungsalgorithmen dar, deren Ziel ist, nach der Parametervorgabe einer globalen Modelleigenschaft (z.B. zulässiges betriebliches Risiko oder tolerierbare Hazardrate) die optimalen Werte der lokalen Parameter (z.B. Ausfallraten, Diagnoseintervalle usw.) herauszufinden.
Schließlich wäre der Anwender bestimmt sehr daran interessiert wenn die Suche nach den optimalen lokalen Parametern auch die entsprechenden Kostenverhältnisse berücksichtigen würde. Eine Integration der Kostenfunktionen in die *PROFUND*-Modellierung stellt eine Basis dieser Weiterentwicklung dar.

Literaturverzeichnis

[2004/49/EC 2004] 2004/49/EC (2004). *Safety Directive 2004/49/EC*. European Parliament and Council of 29th April 2004.

[AEG] AEG. *Allgemeines Eisenbahngesetz*.

[AEIF 2002] AEIF (2002). Association Européenne pour l'Interoperabilité Ferroviaire, http://www.aeif.org/.

[Arabestani 2005] Arabestani, S. (2005). *Formal verifizierbare objektorientierte Systemspezifikation mit UML für Eisenbahnsicherungssysteme*. Doktorarbeit, Technische Universität Braunschweig.

[Bearfield 2005] Bearfield, G. (2005). *D1.3.2. Common Safety Methods: Position Paper*. SAMNET Thematic Network, www.samnet.info.

[Bitsch et al. 2004] Bitsch, F., S. Arabestani und J.-T. Gayen (2004). *Precise Definition of the Single-Track Level Crossing in Radio-Based Operation in UML Notation and Specification of Safety requirements*. In: Ehrig, H., Hrsg.: *Integration of Software Specification Techniques for Applications in Engineering*, Bd. LNCS, S. 119–144. Springer-Verlag, 3147 Aufl.

[Braband 2005] Braband, J. (2005). *Risikoanalysen in der Eisenbahn-Automatisierung*. Eurailpress.

[Braband und Lenartz 2000] Braband, J. und K. Lenartz (2000). *Risikoorientierte Aufteilung von Sicherheitsanforderungen - ein Beispiel*. Signal + Draht, (1+2):5–10.

[Braband und Lennartz 1999] Braband, J. und K. Lennartz (1999). *Systematisches Verfahren zur Festlegung von Sicherheitszielen*. Signal + Draht, S. 5–10.

[Braband und Lennartz 2003] Braband, J. und K. Lennartz (2003). *Experience with Quantified Safety Analysis*. Signal + Draht, S. 23–27.

[Buchacker 2000] Buchacker, K. (2000). *Definition und Auswertung erweiterter Fehlerbäume für die Zuverlässigkeitsanalyse technischer Systeme*. Doktorarbeit, Universität Erlangen-Nürnberg.

[Chalon et al. 1996] Chalon, O., A. Janhsen, S. Röver und E. Schnieder (1996). *Application of advanced systems engineering for train control systems*. In: Allan, J., Hrsg.: *Computers in Railways V*, S. 309–317.

[Cosulich et al. 1995] Cosulich, G., P. Firpo, S. Savio und G. Sciutto (1995). *The Role of Petri Net Modelling in the Safety Assesment Process for Guided Transport Systems*. In: *Applications of Advanced Technologies in Transportation Engineering*, S. 558 – 562.

[Decknatel 2001] Decknatel, G. (2001). *Entwicklung eines Typs kontinuierlich-diskreter höherer Petrinetze und seine Anwendung auf Bahnsysteme*. Doktorarbeit, Technische Universität Braunschweig.

[EBO] EBO. *Eisenbahn-Bau- und Betriebsordnung*.

[Ehrig 2004] Ehrig, H. (2004). *Integration of Software Specification Technique for Applications Engineering*, Bd. 3147. Springer Verlag, LNCS Aufl.

[Einer 2003] Einer, S. (2003). *Petrinetzbasierte Spezifikation und Analyse operationaler Prozesse am Beispiel Eisenbahnsicherung*. Doktorarbeit, Technische Universität Braunschweig.

[EN50126 1996] EN50126 (1996). - *Spezifikation und Nachweis der Verlässlichkeit, Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS)*. Beuth-Verlag.

[EN50128 1999] EN50128 (1999). *EN 50128 - Bahnanwendungen - Software für Eisenbahnsteuerung- und -überwachungssysteme*. Beuth-Verlag.

[EN50129 1998] EN50129 (1998). *EN 50129 - Bahnanwendungen - Sicherheitsrelevante elektronische Systeme für Signaltechnik*. Beuth-Verlag.

[EN50159-1 1999] EN50159-1 (1999). *EN 50159-1 - Bahnanwendungen - Software für Eisenbahnsteuerung- und -überwachungssysteme*. Beuth-Verlag.

[EN50159-2 1999] EN50159-2 (1999). *EN 50159-2 - Bahnanwendungen - Software für Eisenbahnsteuerung- und -überwachungssysteme*. Beuth-Verlag.

[EuroStat 2006] EuroStat (2006). *Eisenbahnunfälle in der Europäischen Union*. http://epp.eurostat.ec.europa.eu/portal.

[Fay und Schnieder 1997] Fay, A. und E. Schnieder (1997). *Knowledge-based decision support system for real-time train traffic control*. In: *Preprints of the 7th International Workshop on Computer-Aided Scheduling of Public Transport CASPT '97*, S. 109–125, Boston.

[Fay und Schnieder 1998] Fay, A. und E. Schnieder (1998). *Information and knowledge valuable assets used for train operation and control*. In: Mellitt, B., R. J. Hill, J. Allan, G. Sciutto und C. A. Brebbia, Hrsg.: *COMPRAIL 98: Computers in Railways VI*, S. 917–927. WIT Press.

[Fenelon et al. 1995] Fenelon, P., J. McDermid, A. Nicholson und D. Pumfrey (1995). *Experience with the application of HAZOP to computer based systems*. In: *Proceedings of the 10th Annual Conference on Computer Assurance*, Gaithersburg, MD. IEEE.

[Garvels und Rubinstein 2001] Garvels, M. und R. Rubinstein (2001). *A Combined RESTART - Cross Entropy Method for Rare Event Estimation with Applications to ATM Networks*. Technischer Bericht, The Faculty of Industrial Engineering and Management, Technion - Institute of Technology.

[German 1994] German, R. (1994). *Analysis of Stochastic Petri Nets with Non-Exponentially Distributed Firing Times*. Doktorarbeit, TU-Berlin.

[Gralla und Heinz 1998] Gralla, D. und S. Heinz (1998). *Fehlermöglichkeits- und Einflußanalyse FMEA*. Eisenbahningenieur, (7).

[Hansen 1996] Hansen, K. M. (1996). *Linking Safety Analysis to Safety Requirements*. Doktorarbeit, University of Denmark.

[Haraszti und Townsend 1999] Haraszti, Z. und J. Townsend (1999). *Rare Event Simulation of Delay in Packet Switching Networks Using DPR-based Splitting*. In: *Winter Simulation Conference*, Pheoenix, Arizona.

[Hänsel et al.] Hänsel, F., J. Poliak, R. Slovák und E. Schnieder. *Reference Case Study "Traffic Control Systems" for Comparison and Validation of formal Specifications Using a Railway Model Demonstrator*. In: Ehrig, H., Hrsg.: *Integration of Software Specification Technique for Applications Engineering*, Bd. 3147, S. 96–119. LNCS Aufl.

[IEC 61025 2003] IEC 61025 (2003). *Störungsbaumanalyse*. DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik. Entwurf.

[IEC 61165 2005] IEC 61165 (2005). *Application of Markov techniques*. International standard, IEC technical committee 56.

[IEC65108] IEC65108. *IEC Norm*.

[Janhsen et al. 1997] Janhsen, A., K. Lemmer, B. Ptok und E. Schnieder (1997). *Modelling and simulation of the new European train control system*. In: Troch, I. und F. Breitenecker, Hrsg.: *2nd Mathmod Vienna, IMACS Symposium on Mathematical Modelling*, S. 473–478.

[Kaiser und Gramlich 2004] Kaiser, B. und C. Gramlich (2004). *State-Event-Fault-Trees – A Safety Analysis Model for Software Controlled Systems*. In: Heisel, M., P. Lyggesmeyer und S. Wittmann, Hrsg.: *Computer Safety, Reliability, and Security*, LNCS. Springer Berlin / Heidelberg.

[Kassev et al. 2006] Kassev, K., R. Slovák, E. Ivanov, N. Stoytcheva und E. Schnieder (2006). *An Application of Phase-Type Distribution for Modelling of Railway Safety-Critical Systems*. In: *Žel 2006*, S. 148–159, Žilina. Universität Žilina.

[Klose 2003] Klose, J. (2003). *Live Sequence Charts: A Graphical Formalism for the Specification of Communication Behaviour*. Doktorarbeit, Carl von Ossietzky Universität Oldenburg.

[Knewitz 2005] Knewitz, R. (2005). *5. Internationaler SIGNAL+DRAHT-Kongress 2005*. Signal + Draht, S. 6–16.

[Koch 2005] Koch, T. (2005). *Heutige Vorgehensweise nach CENELEC - Welche Fragen bleiben trotz der Application Guides noch offen?*. In: *Signal + Draht Kongress "Eisenbahnsicherheit: Europa stellt neue Anforderungen"*, Fulda.

[Kuhlmann 1981] Kuhlmann, A. (1981). *Einführung in die Sicherheitswissenschaft*. Vieweg and Sohn Verlag TÜV Rheinland.

[Leveson und Stolzy 1987] Leveson, N. G. und J. I. Stolzy (1987). *Safety Analysis Using Petri Nets*. IEEE Transactions on Software Engineering.

[Luttenberger und Cramer 1992] Luttenberger, C. und A. Cramer (1992). *Messung, Modellierung und Bewertung von Echtzeitsystemen, Methodik und Fallstudie*. In: *Petrinetze in der Automatisierungstechnik*, S. 180–211. Oldenbourg-Verlag, München.

[Marsan et al. 1995] Marsan, M. A., G. Balbo, G. Conte, S. Donatelli und G. Franceschinis (1995). *Modelling with Generalized Stochastic Petri Nets*. John Wiley and Sons, Chichester.

[Meyer zu Hörste 2003] Meyer zu Hörste, M. (2003). *Methodische Analyse und generische Modellierung von Eisenbahnleit- und -sicherungssysteme*. Doktorarbeit, Technische Universität Braunschweig.

[Meyer zu Hörste et al. 2000] Meyer zu Hörste, M., B. Ptok, E. Schnieder und H. Schrom (2000). *A Case Study for the Automated System Development: The Satellite-based Train Control System*. In: *Control Systems Design CSD 2000*, S. 329–334.

[Meyer zu Hörste et al. 1998] Meyer zu Hörste, M., B. Ptok, E. Schnieder und H.-M. Schulz (1998). *Modelling and Simulation of the European Train Control System for Testcase Spezification*. In: Mellitt, B., R. Hill, J. Allan, G. Sciutto und C. Brebbia, Hrsg.: *COMPRAIL '98 - Computers in Railways VI*, S. 649–658.

[Meyer zu Hörste und Schnieder 1999] Meyer zu Hörste, M. und E. Schnieder (1999). *Formal Modelling and Simulation of Train Control Systems using Petri Nets*. In: J. Wing, J. Woodcock, J Davies, Hrsg.: *World Congress on Formal Methods in the Development of Computing Systems*, S. 1867.

[Michalewicz und Fogel 2000] Michalewicz, Z. und D. Fogel (2000). *How to solve it: Modern Heuristics*. Springer.

[Montigel 1996] Montigel, M. (1996). *Modellierung und Gewährleistung von Abhängigkeiten in Eisenbahnsicherungsanlagen*. Doktorarbeit, Eidgenossische Technische Hochschule Zürich.

[Mueller und Schnieder 2006] Mueller, L. und E. Schnieder (2006). *Prozessoptimierung als Beitrag zur Sicherheitskultur in der Eisenbahnindustrie*. ETR, (10).

[Ortmeier 2005] Ortmeier, F. (2005). *Formale Sicherheitsanalyse*. Doktorarbeit, Universität Augsburg.

[Petri 1962] Petri, C. A. (1962). *Kommunikation mit Automaten*. Doktorarbeit, TH Darmstadt.

[Pope et al. 2006] Pope, M., J. Drewes und J. May (2006). *Generic Hazard List for Railway Systems*. In: *7th World Congress on Railway Research*, Montreal.

[Pozsgai und Bertsche 2005] Pozsgai, P. und B. Bertsche (2005). *Modeling and Simulation of the operational availability and costs of complex systems - a case study*. In: *ESREL*, S. 1597–1605, Gdansk.

[prTR50126-2 2005] prTR50126-2 (2005). *Railway Applications - The Specification and Demonstartion of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Guide to the application of EN 50126 for Safety*. CENELEC, Brussels. First Draft.

[Rackwitz 2003] Rackwitz, R. (2003). *Risk perception and rational risk control management in our natural and technical environment*. In: *JCSS-WP2*, Paris.

[Reifer 1979] Reifer, D. (1979). *Software failure modes and effects analysis*. IEEE Transactions on Reliability, 28(3).

[Schneeweiss 1999] Schneeweiss, W. (1999). *Petri Nets for Reliabilty Modelling*. LiLoLe-Verlag, Hagen.

[Schnieder 1996] Schnieder, E. (1996). *Betriebsleittechnik für die Magnetschnellbahn TRANSRAPID*. at - Automatisierungstechnik, S. 428–436.

[Schnieder 1998] Schnieder, E., Hrsg. (1998). *FORMS 1998 - Formale Techniken für die Eisenbahnsicherung*. Institut für Regelungs- und Automatisierungstechnik, TU Braunschweig, Fortschritt-Berichte VDI.

[Schnieder 1999a] Schnieder, E., Hrsg. (1999a). *FORMS 1999 - Formale Techniken für die Eisenbahnsicherung*. Institut für Regelungs- und Automatisierungstechnik, TU Braunschweig, Fortschritt-Berichte VDI.

[Schnieder 1999b] Schnieder, E. (1999b). *Methoden der Automatisierung*. Vieweg Verlag.

[Schnieder 2000] Schnieder, E., Hrsg. (2000). *FORMS 2000 - Formale Techniken für die Eisenbahnsicherung*. Institut für Regelungs- und Automatisierungstechnik, TU Braunschweig, Fortschritt-Berichte VDI.

[Schnieder 2003] Schnieder, E. (2003). *Beschreibung der Verlässlichkeit von Verkehrssystemen im Verfügbarkeits-Sicherheits-Diagramm*. Signal + Draht, (10):6–9.

[Schnieder und Bikker 1998] Schnieder, E. und G. Bikker (1998). *An Integrated Resource Model for Automation Systems*. In: *17th IASTED International Conference Modelling, Identification and Control*.

[Schnieder et al. 2005] Schnieder, E., R. Slovák und S. Wegele (2005). *New and Conventional Measures for Quantifying Risk in Rail Transport*. Journal of System Safety Society, (41(1)).

[Schnieder und Tarnai 2004] Schnieder, E. und G. Tarnai, Hrsg. (2004). *FORMS/FORMAT 2004 - Formal Methods for Railway Operation and Automation Systems*.

[Slovák et al. 2005] Slovák, R., S. Wegele und E. Schnieder (2005). *Ein Auswertungsverfahren für Verlässlichkeitsanalysen in der Bahntechnik*. In: *Tagung der technischen Zuverlässigkeit*, S. 213–228, Stuttgart. VDI.

[Smith 2006] Smith (2006). *Level crossing safety performance report*. Technischer Bericht, Rail Safety and Standards Board, London.

[SPNP] SPNP. *URL: http://www.ee.duke.edu/ kst/*.

[Stanley und Stutzbach 2006] Stanley, P. und J. Stutzbach (2006). *Optimierung von Kosten und Sicherheit durch geeignete Nutzung der EN*. Signal + Draht, S. 35–38.

[Starke 1990] Starke, P. H. (1990). *Analyse von Petri-Netz-Modellen*. B. G. Teubner Stuttgart.

[Stoytcheva et al. 2005] Stoytcheva, N., K. Kassev, R. Slovák und E. Schnieder (2005). *Quantitative RAMS Modelling and Analysis with Markov Chains and Stochastic Petri Nets*. In: *Žel 2005*, S. 219–229, Žilina. Universität Žilina.

[Tarnai und Schnieder 2003] Tarnai, G. und E. Schnieder, Hrsg. (2003). *FORMS 2003 - Formal Methods for Railway Operation and Control Systems*. L'Harmattan Budapest.

[Thums 2004] Thums, A. (2004). *Formale Fehlerbaumanalyse*. Doktorarbeit, Universität Augsburg.

[TimeNET] TimeNET. *URL: http://pdv.cs.tu-berlin.de/ timenet/*.

[Trivedi et al. 1993] Trivedi, K. S., G. Ciardo, M. Malhotra und R. A. Sahner (1993). *Dependability and Performability Analysis*. In: *Lecture Notes in Computer Science vol. 729*. Springer.

[Trost et al. 2005] Trost, M., S. Nebel, P. Pozsgai und B. Bertsche (2005). *Modellierung komplexer Systeme mit Hilfe stochastischer Netzverfahren*. In: *TTZ - Tagung Technischer Zuverlässigkeit*, S. 185–198, Stuttgart. VDI.

[VDI3682 2002] VDI3682 (2002). *Formalisierte Prozessbeschreibungen*. Düsseldorf.

[Vesely et al. 1981] Vesely, W. E., F. F. Goldberg, N. H. Roberts und D. F. Haasl (1981). *Fault Tree Handbook*. Washington, D.C.

[Vijendran et al. 2004] Vijendran, M., M. Beard und S. Arthur (2004). *Red light violations at level crossings*. In: *8th International Level Crossing Symposium*, Sheffield. RSSB.

[Wittenberg 2002] Wittenberg, K. D. (2002). *Sicherheits- und Betreiberverantwortung im Eisenbahnbetrieb - Teil 1*. Signal + Draht, S. 37–42.

[Zahradník et al. 2004] Zahradník, J., K. Rástočný und M. Kunhart (2004). *Sicherheit der Eisenbahnsicherungssystemen*. EDIS Žilinská Univerzita. (auf slowakisch).

[Zhu 2001] Zhu, P. (2001). *Betriebliche Leistung von Bahnsystemen unter Störungsbedingungen*. Doktorarbeit, Technische Universität Braunschweig.

[Zhu und Schieder 2000b] Zhu, P. und E. Schieder (2000b). *Holistic Modelling of complex Systems with Petri Nets*. In: *IEEE International Conference on Systems, Man and Cybernetics (SMC 2000)*, S. 3075–3080, Nashville.

[Zhu und Schnieder 2000a] Zhu, P. und E. Schnieder (2000a). *Modelling and Performance Evaluation of Railway Traffic under Stochastic Disturbances*. In: *Transportation Systems 2000*, S. 289–294, Braunschweig.

[Zimmermann 1997] Zimmermann, A. (1997). *Modellierung und Bewertung von Fertigungssystemen mit Petrinetzen*. Doktorarbeit, TU Berlin.

[Zimmermann et al. 1999] Zimmermann, A., H. Westphal und S. Gramlich (1999). *Colored Petri Nets for the Performance Evaluation of a Semiconductor Fabrication Facility*. In: *7th Int. IEEE Conf. on Emerging Technologies and Factory Atutomation (ETFA'99)*, Barcelona.